



**NATO UNCLASSIFIED**

7 January 2013

**DOCUMENT**  
AC/35-D/2000-REV7

**SECURITY COMMITTEE**

**DIRECTIVE on PERSONNEL SECURITY**

**Note by the Chairman**

1. At Annex is the seventh revision of the Directive on Personnel Security which is published in support of the NATO Security Policy, C-M(2002)49. It is binding and mandatory in nature upon NATO member nations, commands and agencies. This document replaces AC/35-D/2000-REV6 which should be destroyed.
2. This revision reflects approved changes concerning NATO PSC Templates which are contained in Appendices 1 and 2.
3. This document has been approved by the Security Committee in Security Policy Format (AC/35-DS(2012)0005-AS1 (SP) and AC/35-WP(2012)0004-REV1 (SP) refer) and will be subject to periodic review.

(Signed) Stephen F. Smith

Annex: 1

Action Officer: Robert Keil, NOS/POB, Ext. 4084



**NATO UNCLASSIFIED**

**DIRECTIVE ON PERSONNEL SECURITY**

**INTRODUCTION**

1. This Personnel Security directive is published by the Security Committee (AC/35) in support of Enclosure "C" to NATO Security Policy (C-M(2002)49). This directive contains mandatory provisions and also includes information which clarifies the meaning of those provisions. This directive addresses the following aspects :

- (a) personnel security clearances:
  - (i) responsibilities;
  - (ii) the requirements for identifying positions requiring an appropriate personnel security clearance (PSC);
  - (iii) the criteria for assessing eligibility for a PSC;
  - (iv) the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET security clearances;
  - (v) the requirements for the provision of PSCs to employees of NATO civil and military bodies;
  - (vi) the requirements for the revalidation of PSCs;
  - (vii) the procedures for addressing adverse information about an individual holding a PSC; and
  - (viii) the requirements for maintaining records of PSCs granted to individuals;
- (b) security awareness and briefing of individuals;
- (c) authorising access to NATO classified information – provisional appointments, one-time access, emergency access, and attendance at conferences and meetings;
- (d) personnel security clearances for couriers, guards and escorts; and
- (e) access by non-NATO nationals.

**PERSONNEL SECURITY CLEARANCE (PSC)**

2. In accordance with the requirements of NATO Security Policy, there shall be an agreed standard of confidence about the loyalty, trustworthiness and reliability of all individuals granted access to, or whose duties or functions may afford access to, NATO classified information. In order to achieve this, individuals authorised to have access to information classified NC or above shall hold an appropriate personnel security clearance (PSC), valid for the duration of the authorised access, and have a need-to-know. Specifically:

- (a) individuals hired directly by NATO civil and military bodies shall be granted a NATO Personnel Security Clearance (PSC) by the National Security Authority (NSA) or other competent authority of the individual's parent government;
- (b) individuals who are employed by a military or civil agency of their government and who are seconded to a position for employment with a NATO civil or military body shall also be granted a NATO PSC by the NSA or other competent authority of the individual's parent government;
- (c) individuals who are employed by a member nation or who are assigned by a member nation to its national delegation at NATO HQ must have been granted an appropriate and valid national and/or NATO PSC; and
- (d) individuals who are contractors shall be granted a NATO Personnel Security Clearance (PSC) by the National Security Authority (NSA) or other competent authority. Further guidance concerning contractors can be found within Enclosure "G" to C-M(2002)49, and the supporting Directive on Industrial Security.

**Responsibilities**

3. NSAs or other competent national authorities are responsible for :

- (a) carrying out security investigations on their nationals / citizens<sup>1</sup>, and other persons within their jurisdiction, who require access to information classified NC or above, and for determining whether a PSC should be granted, denied or revoked. Standards of investigation shall be in accordance with the national investigative practices of NATO nations, but in no case shall these standards be lower than those prescribed in paragraphs 7 to 10 below;
- (b) ensuring that PSC procedures are carried out with the knowledge and consent of the individual being investigated, to the extent that is permitted by national legislation;
- (c) revalidating PSCs; and
- (d) co-operating with other NSAs or other competent national authorities in carrying out their respective PSC procedures.

<sup>1</sup> There is provision in the industrial security context (Ref.: Directive on Industrial Security, Para: 43, 44) for a NSA/DSA to grant a PSC to an individual holding the nationality / citizenship of another NATO nation.

4. NATO nations and the Heads of a NATO civil or military body are responsible for :
- (a) identifying positions which require a PSC;
  - (b) authorising access to NATO classified information within their area of responsibility, including the situations described in paragraphs 28 to 37 below;
  - (c) ensuring that personnel security standards, as set forth herein, are met; and
  - (d) evaluating continuing eligibility of their staff for access to NATO classified information.

**Identifying Positions Requiring a Personnel Security Clearance (PSC)**

5. In order to assess whether a position requires a PSC, NATO nations and NATO civil and military bodies shall involve managers who will be the most familiar with the work of their staff and the levels of access to NATO classified information the position requires. It is they who will generally be the best judge of the security clearance level required for the position.

6. Managers shall also be responsible for ensuring that their staffs have the level of PSC appropriate to the access that their work requires and that the principle of need to know is applied. When an individual's PSC is due for its regular 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**

7. The following paragraphs contain the principal 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 character and circumstances which may give rise to potential security concerns.

8. Although the criteria apply to the individual being cleared, 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 clearance.

9. The criteria shall be applied to determine if an individual or his spouse, co-habitant, and where appropriate and in accordance with national legislation, 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 nations, including intelligence services of foreign nations, which may threaten the security of NATO and/or NATO nations, 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 the member nations, or a change in the form of government of the member nations;
- (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 deliberately withheld, misrepresented or falsified information of significance, particularly of a security nature, or has deliberately lied in completing the personnel security form or during the course of a security interview;
- (f) has been convicted of a criminal offence, or offences indicating habitual criminal tendencies; or has serious financial difficulties or unexplained affluence; or has a history of alcohol dependence, use of illegal drugs and/or misuse of legal drugs;
- (g) is or has been involved in conduct, including any form of sexual misconduct, which may give rise to the risk of vulnerability to blackmail or pressure;
- (h) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;
- (i) has seriously or repeatedly infringed security regulations; or has attempted, or succeeded in, unauthorised activity in respect to communication and information system(s);
- (j) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in his judgement or reliability or may make the individual, unintentionally, a potential security risk. In all such cases competent medical advice should be sought; or
- (k) may be liable to pressure through relatives or close associates who could be vulnerable to foreign intelligence services, terrorist groups or other subversive organisations or individuals whose interests may threaten the security interests of NATO and/or NATO nations.

### Dual Nationals

10. For individuals holding dual-nationality, one of which may be non-NATO, special attention should be afforded when considering eligibility for a security clearance. Provided that the parent nation NSA<sup>2</sup> granting the clearance is content that there is no actual or potential conflict of loyalty, there is no prima facie reason to deny a clearance.

---

<sup>2</sup> There is provision in the industrial security context (Ref.: Directive on Industrial Security, Para: 43, 44) for a NSA/DSA to grant a PSC to an individual holding the nationality / citizenship of another NATO nation.

**Investigative Requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET Clearances**

11. The initial security clearance for access to information classified NC and NS 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 **Personnel Security Questionnaire** (which can be either NATO or national);
- (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 shall 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 law enforcement agencies with legal jurisdiction where the individual has resided or been employed for at least six months shall be checked.

12. The initial security clearance for access to information classified CTS 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 11 above, the following are required for clearances for access to information classified CTS; these factors may also be relevant to the assessment of NC and NS clearances, where they are compliant with national rules and legislation :

- (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 18<sup>th</sup> birthday, or during an appropriate period as judged by the investigating security authority, at schools, 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:** where provided and admissible under national law :
- (i) interview(s) shall also be conducted with the individual especially if the initial enquiries have revealed potentially adverse information; and
  - (ii) interviews shall also be conducted with individuals 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.

13. Lack of coverage in any investigative category shall be compensated for through other investigative means, in accordance with National security rules and regulations.

#### **Granting a Personnel Security Clearance**

14. The NSA or competent national authority shall consider all available information in order to determine whether a PSC shall be granted or not. It should be noted that 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 NSA or competent national authority shall assess the risks associated with each case in order to determine whether a clearance may be granted.

#### **Security Clearance Certificate for Employees of NATO Civil and Military Bodies**

15. Once a NSA or other competent national authority has granted a PSC to an individual to be employed by, or seconded, to a NATO civil or military body, or an individual assigned by a member nation to its national delegation at NATO HQ, they shall either directly, or upon specific request by the respective NATO body, provide a copy of a PSC certificate to the NATO civil or military body at which the individual is to take up his appointment. An example of this certificate is provided at Appendix 1. In all cases, the date on which the security clearance was granted, and the date of validity of the security clearance shall appear on the personnel security clearance certificate.

16. If an individual's period of service does not commence within 12 months of the issue of a new PSC to fill a post with a NATO civil or military body, or if there is a break of 12 months in an individual's service, during which time he is not employed in a position with a NATO or a NATO member government civil or military body, the PSC shall be referred to the individual's parent NSA for confirmation that it remains valid and appropriate.

#### **Security Clearances for Contractor Personnel Performing Works for NATO Civil or Military Bodies**

17. The provision for Personnel Security Clearances or the confirmation of those for contractor personnel performing works on NATO premises and requiring a Personnel Security Clearance is addressed in the Directive on Industrial Security.

**Revalidation of a Personnel Security Clearance**

18. After the initial granting of a PSC and provided the individual has had unbroken service with a NATO nation or NATO civil or military body and has a continuing need for access to NATO classified information, the PSC shall be reviewed for revalidation at intervals not exceeding 5 years for a CTS clearance and 10 years for NS and NC clearances, with effect from the date of the last investigative action on which it was based. All investigations for the renewal of a PSC shall cover the period since the previous investigation. Requests for revalidation of a PSC shall be applied for in a timely manner, in accordance with the requirements of the NSA(s).

19. For revalidation of an NC and NS PSC, the procedures outlined below shall, as a minimum, be carried out :

- (a) the completion of a personnel security questionnaire by the individual concerned. (The form may be either the NATO supplementary personal particulars form or a similar national form supplied by the relevant national authority);
- (b) for individuals employed by a NATO civil or military body, a check of the personnel security questionnaire against the security and personnel records of the NATO body;
- (c) when a revalidation is requested by a NATO civil or military body for individuals employed by a NATO body, the completed personnel security questionnaire mentioned at (a) above and the results of the check required at (b) above, shall be sent to the individual's parent and the host nation NSA;
- (d) review by the nation in which the NATO body is located (i.e., the host nation) of its national records at the request of the individual's parent NSA;
- (e) where applicable, reviews identical with those in (d) above by any other NATO nation in which the staff member has resided if so requested by the parent NSA; and
- (f) when the relevant NATO civil or military body requests the individual's parent NSA to re-validate the security clearance, it shall also pass details of the individual's security record during his/her employment for the period under review.

20. The parent NSA shall then review any information arising during the course of these records checks against the background of its own records and send its decision to the requesting NATO civil or military body.

21. The revalidation of a clearance at the CTS level, in addition to the normal review procedures outlined in paragraph 19 above, may include an interview with the individual and shall require the following to cover the 5 years since the last investigation/review :

- (a) where character references are required by member nations who have supplied their own personnel security questionnaire, references shall be taken up in consultation with the NSA of the host nation;
- (b) in the event that a more detailed investigation is required, 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 the 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 nation on behalf of the parent nation arising from any information which may come to light as a result of any action under paragraph 19 and 21(a) to (c) inclusive above;
- (e) the despatch by the NSA of the host nation and of any other member nation in which the subject has resided, of any information developed within the terms of paragraph 19 and 21(a) to (d) inclusive above to the NSA of the parent nation;
- (f) a review by the parent NSA against the background of its own records of any information which has been sent to it within the terms of (e) above; and
- (g) the despatch of the parent NSA's decision, with regard to the renewal of the personnel security clearance certificate, to the requesting NATO civil or military body.

22. If a NATO personnel security clearance is not revalidated within the life of the clearance, a period of a further 12 months may be allowed for the revalidation to be completed, provided that the responsible NSA has commenced the action necessary to revalidate the clearance. If, at the end of this additional 12-month period, the revalidation has still not been completed, the individual shall be moved to duties which do not require a personnel security clearance. If, exceptionally, enquiries cannot be completed within this period of time, and no adverse information has been found, the NSA/DSA concerned may provide the relevant NATO civil or military body with an extension of the validity of the existing security clearance, indicating a date on which a final decision on the revalidation may be anticipated.

### **Adverse Information**

23. 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, their PSC shall be withdrawn and the individuals shall be excluded from access to NATO classified information and from positions where they might endanger security. When the PSC is withdrawn for an individual seconded to, or directly hired by, a NATO civil or military body, a certificate revoking the PSC shall be issued to the NATO body by the parent NSA.

### **Records of Personnel Security Clearances**

24. Records of the PSCs granted to individuals with access to NATO classified information shall be maintained by the NATO member nations and by the employing NATO civil or military body. These records shall contain details of the level, date and validity of the clearance.

**SECURITY AWARENESS AND BRIEFING OF INDIVIDUALS**

25. All individuals employed in positions where they have access to NR information, or hold a clearance for access to NC 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 which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement shall be maintained by the NATO nation or NATO civil or military body authorising access to NATO classified information.

26. All individuals who are authorised access to, or required to handle NATO classified information, shall initially be made aware, and periodically reminded of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with the media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate security authorities any approach or manoeuvre which they consider suspicious or unusual.

27. All individuals who cease to be employed in duties requiring access to NATO classified information shall be made aware of, and acknowledge, their responsibilities for the continued safeguarding of NATO classified information.

**AUTHORISING ACCESS TO NATO CLASSIFIED INFORMATION**

28. An individual shall only be authorised access to NATO classified information after he has been granted the appropriate personnel security clearance, a determination of his need-to-know has been made, and he has been briefed on NATO security procedures and has acknowledged his security obligations.

**Exceptional Circumstances**

**Provisional appointments**

29. 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) the placement of the individual is approved by 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.

30. Provisional appointments shall not extend beyond six months from the date the individual takes up the position. An NSA may extend the appointment for another six months if the investigation has been initiated and there is no adverse information.

**One time Access**

31. Exceptionally, individuals may be authorised access on a one-time basis to NATO information 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 NATO classified information 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) authorisation shall be granted only by an OF6 ("one-star general") or the civilian equivalent, after co-ordination with the appropriate security authority(s); and
- (f) a record of the exception, including a description of the information to which access was approved, shall be maintained by the cognisant security office.

32. This procedure shall not be used on a recurring basis for access to NATO classified information. If this is required, or if access is required for more than 6 months, a personnel security clearance for the higher level must be obtained.

**Access in Exceptional Circumstances**

33. Individuals may, as an exception, be authorised access, to NATO HQ and NATO Civil or Military Bodies' premises and to NATO Classified information, provided that the following criteria are fulfilled:

- (a) individuals are nationals of a NATO Member Nation;
- (b) access shall be authorised by the Head of NATO HQ Division, or NATO Civil or Military Body based on a compelling written justification;
- (c) access shall be limited to specific items of NATO information classified up to and including NATO SECRET in support of the mission described by the Head of a NATO HQ Division, or NATO Civil or Military body;
- (d) access shall be authorised on a one time basis or for a limited period of time, in any case not exceeding six months;
- (e) access shall be limited to administrative zones, or class 2 security areas;
- (f) access to CIS processing NATO classified information shall not be authorised, other than to CIS intended solely to support the activity in which the individual is engaged;

- (g) the responsible parent NSA has granted, in accordance with national legislation, a provisional PSC, or has confirmed that the security clearance process of the individual has already started and that preliminary records checks have not revealed adverse information; and
  - (h) a record of the exceptions, including a description of the facility and of the information to which access was approved, should be maintained by the responsible Security Office and should be periodically forwarded to the NOS.
34. The procedure described in paragraphs 33 and 35 shall be limited to the following cases:
- (a) Short Term employment of an individual whose capacity, with respect to the activity, makes him indispensable;
  - (b) Employment of interpreters, both from NATO and non-NATO Nations.

The procedure shall not be used on a recurring basis for access to NATO premises, or to NATO classified information. To this end, NOS shall maintain records of the exceptions and inform the NSC accordingly.

#### **Employment of Interpreters from Non-NATO Nations**

35. Employment of interpreters who are not nationals of a NATO member nation may be permitted as an exception in the following cases:
- (a) the language to be interpreted from/into requires a mother tongue speaker who is not a NATO national; and
  - (b) the NATO classified information to be interpreted shall have been assessed and authorised for release to the parent nation of the interpreter.

The provisions of paragraphs 33 (b)-(c)-(f)-(h) above shall apply.

#### **Emergency Access**

36. 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, member nations and the Heads of NATO civil and military bodies may, in exceptional circumstances, grant by written authorisation, access to NATO classified information to individuals who do not possess the requisite personnel security clearance, provided that such authorisation is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. A record of this authorisation describing the information to which the access was given shall be maintained.

37. In the case of information classified CTS, this emergency access shall be confined wherever possible to those individuals who have been authorised access to either national TOP SECRET or to information classified NS.

**Personnel Security Clearances for Senior Government Officials**

38. Access to NATO classified information by Senior government officials (for example, Heads of State and Government, Government Ministers, Members of Parliament, and members of the Judiciary) is determined by national rules and regulations; such SGOs should be briefed on their security obligations in respect to the protection of NATO classified information.

**Access by Spouses / Dependents to NATO Classified Information**

39. Spouses or dependents of individuals employed by NATO civil and military bodies who are required to have access, on a need-to-know basis, to NATO classified information shall be security cleared, and shall be briefed on their security obligations in respect to the protection of NATO classified information. The security clearance process shall include, as a minimum, the requirements that are established for a personnel security clearance, as stated in paragraphs 11 to 13 above.

**ATTENDANCE AT CONFERENCES AND MEETINGS**

40. An individual's authorisation for participation in a conference, course, meeting or seminar shall be based on the following:

- (a) an identity check and confirmation of the individual's authorisation and security clearance, if required;
- (b) the provision of an Attestation of Personnel Security Clearance as provided in Appendix 2;
- (c) this form shall be issued by NATO civil or military bodies, NSAs or other competent national authority, and be transmitted to the appropriate authorities, or exceptionally be hand carried by the delegates concerned;
- (d) where appropriate and agreed by the receiving and transmitting authorities, a consolidated list of names including the details required in Appendix 2 is acceptable;
- (e) at NATO facilities with national diplomatic or military delegations/representations specific arrangements shall be agreed between the Security Office of the NATO facility and the national delegations/representatives stating that the national delegations / representatives provide to the security office of the NATO facility a confirmation of the appropriate clearance of its national when requesting an access badge to the facility; and
- (f) visits for any purpose by company representatives, consultants or contractors to NATO facilities or establishments shall follow the provisions of Enclosure "G" to the NATO Security Policy C-M(2002)49 and the latest version of its supporting Directive on Industrial Security AC/35-D/2003.

**COURIERS / GUARDS / ESCORTS**

41. Couriers and guards employed to carry documents classified NC and above shall be security cleared, as a minimum, to the NS level by their NSA, unless specific National security rules and regulations are applied. Couriers, guards and escorts shall be briefed on NATO security procedures and shall be instructed on their duties for protecting the NATO classified information entrusted to them. When individuals such as guards and escorts are employed in circumstances where they might have unauthorised access to classified information, they shall be security cleared to the level deemed appropriate by the relevant security authority.

**ACCESS BY NON-NATO NATIONALS**

42. Non-NATO nationals serving as integrated members of the Armed Forces of NATO member nations may be authorised access up to and including information classified CTS. In the case of such nationals it shall be incumbent upon the NATO member nation NSA to satisfy itself that the conditions for security clearance and access required by this directive and NATO Security Policy are fulfilled.

43. In accordance with the overall provisions of NATO Security Policy, individuals who are nationals<sup>3</sup> of non-NATO nations or who are individuals from an international organisation may be granted access to NATO classified information on a case-by-case basis, provided that :

- (a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;
- (b) the individual is granted a NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives; noting that a NATO PSC is not required for access to NR information;
- (c) the prior written consent of the NATO nation or NATO civil or military body that originated the information is obtained; and
- (d) the non-NATO individual in question shall have clearly understood and undertaken, by means of personally undersigning an acknowledgement of responsibilities, that NATO information that he might have access to in the context of a specified NATO programme, project, contract, operation, or related task, shall strictly and solely be used for the purposes of the entrusted task and shall not be shared with or transmitted to third persons, bodies, organisations or governments.

---

3

Nationals of non-NATO nations includes "nationals of a Kingdom", "citizens of a State", and "landed immigrants in Canada". "Landed immigrants in Canada" are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.

44. As an exception to the requirement for originator control in sub-paragraph 43(c) above, NSAs of NATO nations may approve access to NATO classified information by nationals of certain non-NATO nations who are employed by NATO Civil or Military Bodies, the Government of the NATO nation, or by a contractor that is located and incorporated in the NATO nation, provided that all of the following criteria are met, in addition to those in sub-paragraphs 43(a), 43(b) and 43(d) above :

- (a) disclosures shall be limited to individuals who are nationals of the following countries - Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland. NSAs may propose changes to the list of countries, for consideration by the NSC;
- (b) access shall be limited to information that is classified no higher than NS, and in accordance with any dissemination limitation or administrative marking that has been applied by the originator. Access shall not be provided to CTS information, ATOMAL or other Special Category information;
- (c) the non-NATO national shall be granted access to the NATO classified information only for the period of time necessary to provide the specified support to a NATO project, programme, contract, operation or related task. The control of access to the NATO classified information shall be the ultimate responsibility of the security officer of the facility or organisation at which access is provided; the security officer shall be a national of a NATO member nation;
- (d) access to the information shall be for the original purpose for which the information was provided to NATO;
- (e) there shall be a security of information arrangement or security agreement between the Government of the NATO nation wishing to provide access to the information and the Government of the nation of citizenship of the non-NATO individual. Moreover, the NATO nation that is to provide access to the information shall ensure, within its national legislation, that it has sufficient control and jurisdiction over the non-NATO national to enable it to prosecute the non-NATO national and hold him accountable for the proper handling of NATO classified information. The NATO Nation may act as a Sponsor in respect of non-NATO nationals employed by NATO Civil or Military Bodies, as required; and
- (f) the NATO nation that is to provide access to the information shall be willing to provide access to its own classified information of a similar type and classification level to the nation of citizenship of the non-NATO national.

**NATO PERSONNEL SECURITY CLEARANCE CERTIFICATE**

1. Certification is hereby given that:

Full Name:

.....

Date and Place of Birth:

.....

has been granted a personnel security clearance by the Government of:

.....

in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is, therefore, declared suitable to be entrusted with information classified up to and including: <sup>4</sup>

.....

.....

2. The validity of this certificate will expire not later than: <sup>5</sup>

.....

Signed:

Title: Official government stamp

Date of Issue:

Contact details of the issuing authority (Phone, e-mail, fax):

.....

<sup>4</sup> Insert, as appropriate, one or more of the following:

- |                       |                              |
|-----------------------|------------------------------|
| (a) COSMIC TOP SECRET | (d) COSMIC TOP SECRET ATOMAL |
| (b) NATO SECRET       | (e) NATO SECRET ATOMAL       |
| (c) NATO CONFIDENTIAL | (f) NATO CONFIDENTIAL ATOMAL |

<sup>5</sup> The date of expiry shall conform with the provisions of paragraph 18 of the Directive on Personnel Security.

<sup>(\*)</sup> The marking is not part of the template.



**ATTESTATION OF NATO PERSONNEL SECURITY CLEARANCE**

1. Attestation is hereby given that:

Full Name .....

Date of Birth .....

Place of Birth .....

Nationality .....

Where employed .....

Purpose and Duration of Visit .....

.....

.....

Holder of Passport/Identity Card No. ....

Issued at ..... Dated .....

Military Rank and Number (where applicable) .....

.....

has been granted access to NATO information classified up to and including  
..... in accordance with current  
NATO security regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL  
information, and has been briefed accordingly by

.....

Signed:

Title: Official stamp

Date of Issue:

2. The validity of the attestation will expire no later than:

.....

3. Issued by .....

(Member nation or NATO civil or military body)

Date and Place of Issue:

.....

Contact details of the issuing authority (Phone, e-mail, fax):

.....

<sup>(\*)</sup> The marking is not part of the template.

PUBLICLY DISCLOSED - AC/35-WP(2010)0003 - MISE EN LECTURE PUBLIQUE