NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

25 November 2020

DOCUMENT
AC/35-D/2000-REV8

SECURITY COMMITTEE

DIRECTIVE ON PERSONNEL SECURITY

Note by the Acting Chair

1. At Annex 1 is the eight revision of the Directive on Personnel Security which is published in support of the Security Within the North Atlantic Treaty Organization, C-M(2002)49-REV1. It is binding and mandatory in nature. This document replaces AC/35-D/2000-REV7 which should be destroyed.

2. The revision is a result of the Comprehensive Review of NATO Security Policy (AC/35-N(2015)0025-AS1, dated 21 December 2015).

3. This document has been approved by the Security Committee (AC/35-N(2020)0004-AS1, dated 4 November 2020) and will be subject to periodic review.

(Signed) Marco Criscuolo

Annex: 1

Action Officer: M. Rožaj, NOS (Ext.: 4084)
Original: English

DIRECTIVE ON PERSONNEL SECURITY
TABLE OF CONTENTS

The following Appendices to this Directive address the specific procedures, arrangements, and sample documents:

(a) APPENDIX 1 - Request for Personnel Security Clearance Confirmation

(b) APPENDIX 2 - Personnel Security Clearance Confirmation

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 (PSCs);

(b) responsibilities with respect to personnel security;

(c) assessing eligibility for a PSC;

(d) investigative requirements for NATO CONFIDENTIAL (NC), NATO SECRET (NS) and COSMIC TOP SECRET (CTS) security clearances;

(e) standards and procedures for a renewal of a PSC;

(f) standards and procedures for addressing adverse information about an individual holding a PSC;

(g) records and means of confirmation as to whether an individual is in possession of an appropriate PSC;

(h) aftercare, security education and awareness;

(i) access to NATO Classified Information in exceptional circumstances; and

(j) access to NATO Classified Information by non-NATO citizens employed by NATO Nations’ civil or military bodies.

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 information classified NC or above. In order to achieve this, individuals who require access or may have access to information classified NC or above during the course of their duties shall have a PSC, at the appropriate level, which is valid for the duration of the authorised access. In addition, such individuals are required to:

(a) have a need-to-know;

(b) have been briefed on their security obligations in respect to the protection of NATO Classified Information; and

(c) have acknowledged their responsibilities either in writing or an equivalent method which ensures non-repudiation.

3. A PSC will be based on a security investigation process that is in full compliance with NATO Security Policy, along with confirmation from the appropriate National Security Authority (NSA) / Designated Security Authority (DSA) or any other competent security authority that the individual in question may be authorised to access NATO Classified Information.

4. Circumstances may arise when some of the requirements above cannot be met. In such instances the procedures for access to NATO Classified Information in exceptional circumstances (as per paragraphs 40 to 48) can be applied.

5. A PSC is not required by NATO Security Policy for access to information classified NATO RESTRICTED (NR). Individuals who only require access to information classified NR shall be briefed on their security obligations and shall have a need-to-know. In accordance with national laws and regulations the individuals shall have acknowledged their security responsibilities in writing or an equivalent method which ensures non-repudiation.

PSCs for Senior Government Officials

6. Access to NATO Classified Information by Senior Government Officials (SGOs) (for example, Heads of State and Government, Government Ministers, Members of Parliament, and members of the Judiciary) is determined by national laws and regulations; such SGOs shall be briefed on their security obligations and shall have a need to know. The SGO's parent NSA/DSA or other competent security authority[1] can be consulted if there is a need to determine whether an SGO can be granted access to NATO Classified Information without a PSC.

PSCs for Contractor Personnel Performing Works for NATO Civil or Military bodies

7. The provision for PSCs or the confirmation of those for Contractor personnel performing work on NATO premises and requiring a PSC is addressed in the Directive on Classified Project and Industrial Security (AC/35-D/2003).

Confirmations of PSCs

8. In situations when an individual will attend or participate in an activity requiring access to NATO Classified Information at the level of NC and above (e.g. conference, meeting, course, seminar), a confirmation of the existence of the individual's PSC is required.

9. Confirmation of the existence of an individual's PSC shall be communicated through official channels (e.g. NSA/DSA to NATO Civil and Military body) and shall only be hand-carried by the concerned individual in exceptional circumstances. NATO Nations and NATO Civil and Military bodies can confirm the existence of individual's PSC by one of the following methods:

(a) a Personnel Security Clearance Confirmation, a template of which is provided in Appendix 2;

(b) a Request for Visit (RfV), in accordance with the provisions of the Directive on Classified Project and Industrial Security (AC/35-D/2003); or

(c) exceptionally, when timely confirmation of an individual's PSC is of paramount importance for the execution of the mission, by other means communicated directly between the NSA/DSA or other competent security authority and the Security Offices of the NATO Civil and Military bodies.

10. The Supporting document on national PSC procedures and requirements (AC/35-D/1043) provides a list of competent security authorities (and their contact details) to be used when confirming that the individual in question is cleared to access NATO Classified Information at the level of NC and above.

11. If an individual's PSC is revoked, suspended or altered (e.g. change in its validity or level), the responsible NATO Nation and**/**or NATO Civil and Military body shall inform all recipients of that individual's PSC confirmation of this change.

[1] As delegated by the NSA/DSA and listed in the Supporting document on national PSC procedures and requirements (AC/35-D/1043).

Confirmations of PSCs for individuals working at NATO

12. The existence of an individual's PSC shall be confirmed when an individual is to be employed by, or seconded to, a NATO Civil or Military body, or assigned by a NATO Nation to its national delegation/representation at NATO. This is accomplished by using one of the following methods:

(a) upon specific request by the respective NATO body, by using the Request for Personnel Security Clearance Confirmation template (Appendix 1); or

(b) directly by the NSA/DSA or any other competent authority of a NATO Nation, by using the Personnel Security Clearance Confirmation template (Appendix 2).

13. An individual's parent NSA/DSA or any other competent security authority shall be requested to provide confirmation that their PSC remains valid if:

(a) an individual's period of employment does not commence within 12 months of the issue of a new PSC to fill a post within a NATO Civil or Military body;

(b) there is a break of 12 months in an individual's employment, during which time the individual is not employed in a post with a NATO or a NATO Nation's government civil or military body.

RESPONSIBILITIES

14. NSAs/DSAs or other competent security authorities are responsible for:

(a) carrying out security investigations on their nationals[2], and, subject to their respective national laws and regulations, 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, following the principles set out in this directive;

(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 laws and regulations;

(c) renewing PSCs and verifying their existence;

(d) informing the recipients of a PSC Confirmation in cases of revocation, suspension or any alteration to a PSC; and

(e) co-operating with other NSAs/DSAs or other competent security authorities in carrying out their respective PSC procedures.

15. NATO Nations and the Heads of NATO Civil or Military bodies are responsible for:

(a) identifying posts which require a PSC;

(b) authorising access to NATO Classified Information within their area of responsibility, including the situations described in paragraphs 40 to 48 below;

(c) ensuring that the personnel security standards, as set forth herein, are met;

(d) evaluating the continuing eligibility of their staff for access to NATO Classified Information;

[2] There is provision in the industrial security context (Directive on Classified Project and Industrial Security (AC/35-D/2003)) for an NSA/DSA or other competent security authority to grant a PSC to an individual holding the nationality/citizenship of another NATO Nation.

(e) informing the relevant NSA/DSA when an individual no longer requires a PSC and/or access to NATO Classified Information (Supporting document on national PSC procedures and requirements (AC/35-D/1043) provides a list of Nations requiring such notification);

(f) supporting NSAs/DSAs or other competent security authorities through provision of relevant information to assist in the security clearance process; and

(g) reporting actual or potential security concerns regarding an individual holding a PSC to the relevant security authority, as set out in paragraphs 31, 32 and 38 below.

Identifying Posts Requiring a PSC

16. In order to assess whether a post requires a PSC, NATO Nations and NATO Civil and Military bodies shall involve the management who will generally be the best judge of the security clearance level required for the post.

17. Management shall also be responsible for ensuring that their staff have the PSC level required to access and complete their work and that the need-to-know principle is applied. When an individual's PSC is due for its regular renewal, or when the post holder changes, the appropriate manager shall be responsible for assessing whether the level of PSC remains necessary for that post.

ASSESSING ELIGIBILITY FOR A PERSONNEL SECURITY CLEARANCE

18. The following are the principal elements for determining the loyalty, trustworthiness and reliability of an individual in order for them to be granted and retain a PSC. These elements consider aspects of character and circumstances which may give rise to potential security concerns and shall be assessed, in accordance with national laws and regulations, to determine if the individual:

(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 organizations 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 organization which by violent, subversive or other unlawful means seeks the overthrow of the government of the NATO Nations, or a change in the form of government of the NATO Nations;

(d) is, or has been, a supporter of any organization or aided or abetted such organizations described in sub-paragraph (c) above, or who is, or who has been closely associated with members of such organizations;

(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 has committed offences indicating habitual criminal tendencies;

(g) has a history of abuse of alcohol;

(h) has a history of use of illegal drugs and/or abuse of legal drugs;

(i) 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;

(j) has demonstrated, by act or through speech, dishonesty, disloyalty, unreliability, untrustworthiness or indiscretion;

(k) has seriously or repeatedly infringed security regulations, or has attempted, or succeeded in, unauthorised activity in respect to Communication and Information System(s) (CIS);

(l) may be vulnerable or liable to pressure, either directly or through relatives or close associates, from foreign intelligence services, terrorist groups or other subversive organizations or individuals whose interests may threaten the security interests of NATO and/or NATO Nations;

(m) has serious financial difficulties or unexplained affluence; and

(n) is suffering, or has suffered, from any illness or mental or emotional condition which may cause significant defects in their judgement or reliability or may make the individual, unintentionally, a potential security risk.

19. Although the criteria above apply to the individual being cleared, where appropriate and in accordance with national laws and regulations, family members and other persons that may have an influence on the individual in question, may also be relevant and should be taken into account when considering that individual's eligibility for a PSC.

Dual Nationals

20. For individuals holding more than one nationality, one of which may be from a non-NATO nation, special attention should be afforded when considering eligibility for a PSC. Provided that the parent nation NSA/DSA or other competent security authority 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.[3]

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

21. 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 their identity checked; citizenship status and/or nationality, past and present, of the individual shall be established and 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 the latter exists, and/or other comparable governmental and police records.

[3] Example: There is provision in the industrial security context (Directive on Classified Project and Industrial Security (AC/35-D/2003) for an NSA/DSA or other competent security authority to grant a PSC to an individual holding multiple nationalities.

22. 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 21 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 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 18th 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:**
(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 background, activities, loyalty, trustworthiness and reliability of the subject of the investigation. 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.

23. Lack of coverage in any investigative category shall be compensated for through other investigative means, in accordance with national laws and regulations. This may include requesting checks from nations where the individual in question has been employed or resided.

Granting a PSC

24. The NSA/DSA or competent security authority shall consider all available information and assess the risks associated with each case in order to determine whether a PSC may be granted. 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) may not be a reason to deny a clearance if the individual's loyalty, trustworthiness and reliability are otherwise undisputed.

25. When a PSC is granted, it shall be valid for a period not exceeding 10 years for access to information classified NC and NS, and not exceeding 7 years for CTS.

Renewal of a PSC

26. The renewal of a PSC shall be initiated prior to the expiration date of the valid PSC. The table in the Supporting document on national PSC procedures and requirements (AC/35-D/1043) lists the lead times when the request for renewal of an individual's PSC should be submitted to the parent NSA/DSA or other competent security authority.

27. For renewal of NC and NS PSCs, 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 renewal 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 nation's NSA/DSA or other competent security authority;

(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/DSA or other competent security authority;

(e) when applicable, reviews identical with those in (d) above by any other NATO Nation in which the staff member has resided, at the request of the parent NSA/DSA or other competent security authority; and

(f) when the relevant NATO Civil or Military body requests the individual's parent NSA/DSA or other competent security authority to renew the security clearance, it shall also provide details of the individual's security record during their employment for the period under review.

28. The parent NSA/DSA or other competent security authority shall review the information provided and undertake any necessary checks required under national laws and regulations. When a decision regarding a PSC has been taken it shall notify the requesting NATO Civil or Military body of the outcome. If the decision is positive a PSC shall be confirmed in accordance with paragraph 9 of this Directive.

29. The renewal of a PSC at the CTS level, in addition to the normal review procedures outlined in paragraph 27 above, may include an interview with the individual and shall require the following to cover the timeframe since the last investigation/review:

(a) character references if required by NATO Nations who have supplied their own personnel security questionnaire;

(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 renewed 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/DSA or other competent security authority 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 27 and 29(a) to (c) inclusive above;

(e) a review by the parent NSA/DSA or other competent security authority against the background of its own records of any information which has been sent to it within the terms of (d) above; and

(f) the confirmation of the parent NSA/DSA or other competent security authority's decision, with regard to the renewal of the PSC, to the requesting NATO Civil or Military body.

30. Exceptionally, if a PSC is not renewed before its expiration date the NATO Civil or Military body employing the individual:

(a) shall request from the individual's parent NSA/DSA or other competent security authority an extension of the current clearance, if permitted under national laws and regulations;[4]

(b) shall request from the individual's parent NSA/DSA or other competent security authority an interim or temporary clearance, if permitted under national laws and regulations;[4] or

(c) may grant continued access to NATO Classified Information provided:

(i) the individual's NSA/DSA or other competent security authority has confirmed that the clearance renewal process is still ongoing;

(ii) the current employing NATO Civil or Military body is willing to accept the risk with the individual's continuous access to NATO Classified Information; and

(iii) the decision to grant access to NATO Classified Information is reviewed every 6 months until the PSC is renewed.[5]

Changes to an individual's PSC

31. Any relevant changes to the individual's PSC shall be communicated by the parent NSA/DSA or other competent security authority to the individual's employing body. Where appropriate, the latter shall ensure that all relevant entities to whom confirmation of the existence of the individual's PSC has been provided are notified of the change to the individual's PSC. If adverse information arises concerning an individual, a decision shall be made by the individual's parent NSA/DSA as to whether they shall continue to hold a PSC.

32. When a PSC is suspended or revoked, this decision shall be immediately communicated to the individual's employing body by the parent NSA/DSA or other competent security authority. The employing body shall exclude the individual from access to NATO Classified Information. In addition, the individual shall be made aware of their continuing responsibility to protect information they had access to and the consequences of failing to do so. An acknowledgement, in writing or an equivalent method which ensures non-repudiation, should be used for such debriefing.

[4] Supporting document on national PSC procedures and requirements (AC/35-D/1043) identifies Nations that can, according to their national laws and regulations, extend the validity of a PSC or issue an interim or temporary PSC.

[5] This review process requires that the employing NATO Civil or Military body contacts the NSA/DSA or other competent security authority to confirm that the PSC renewal process is still ongoing.

Records of PSCs

33. Records of the PSCs granted to individuals with access to NATO Classified Information shall be maintained by the NATO Nations and by the employing NATO Civil or Military body. These records (and confirmations, where applicable) shall contain details of the level, date and validity of the clearance.

Security Education and Awareness

34. All individuals employed in posts where they have access to information classified NR, or have a PSC for access to information classified NC or above, shall be briefed on security procedures and their security obligations in respect to the protection of NATO Classified Information. Individuals shall acknowledge, in writing or an equivalent method which ensures non-repudiation that they fully understand their responsibilities and the possible consequences to them, outlined in their national laws and regulations if they are found to have allowed NATO Classified Information to pass 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.

35. NATO Nations and NATO Civil or Military bodies are responsible for developing an appropriate Security Awareness Programme for all individuals authorised to access NATO Classified Information.[6] It shall be made incumbent upon individuals to undertake security training or other events for the raising of security awareness on a regular basis.

36. Security Education and Awareness shall be tailored to the particular target audience, but should, as a minimum, encompass:

(a) the pertinent regulations, which apply to the protection of NATO Classified Information and the consequences for their violation;

(b) hostile intelligence threats, information collection techniques and methods, as well as defensive measures for countering the threat;

(c) information about most common threats applicable to CIS and about basic end-user protective measures to counter those threats; and

(d) the requirement to report promptly all security violations, unauthorised disclosures or possible compromises of NATO Classified Information to the relevant security authority.[7]

37. All individuals who no longer require access to NATO Classified Information shall be made aware of their continuing responsibility to protect such information and the consequences of failing to do so. In accordance with national laws and regulations, an acknowledgement, in writing or an equivalent method which ensures non-repudiation, should be used for such debriefing.

---

6 Nations may use either NATO specific briefings or national equivalent if the latter highlights the differences between the requirements of the two security frameworks.

7 Additional guidance on development of a comprehensive Security Education and Awareness can be found in the Supporting document on Security Education and Awareness (AC/35-D/1029).

AFTERCARE

38. While the responsibility for assessing the individual's eligibility for a PSC rests with the NSA/DSA or other competent security authority, the ongoing awareness of personnel with regards to the protection of NATO Classified Information is the responsibility of the organization employing the individual in the context of countering the risk of Insider Threat[8]. The employing body shall report relevant security concerns about the individual having a PSC to the NSA/DSA or other competent security authority that issued the individual's PSC in order to determine whether the individual shall continue to have a PSC.

39. In addition, there should be a layered approach of countermeasures[9] in place in order to mitigate the risk of Insider Threat. Such countermeasures should encompass:

(a) effective line management allowing for identifying and addressing behaviour with potential security implications;

(b) good management practices, which increase employees' commitment and loyalty;

(c) performance evaluation process that include addressing any security issues related to the specific individual, post or organization;

(d) robust access control to sensitive areas and CIS to identify any unauthorised activity;

(e) mandatory reporting of changes in the individual's personal circumstances by the individuals holding a PSC, particularly those with a PSC at the CTS level or holding sensitive posts; and

(f) regular security awareness training and establishment of a security culture enforcing strong compliance with security procedures.

ACCESS TO NATO CLASSIFIED INFORMATION IN EXCEPTIONAL CIRCUMSTANCES

Interim or Temporary Clearances

40. In situations where either the initial clearance process has been commenced but not yet completed or an individual's PSC is being renewed, when the parent NSA/DSA or other competent security authority has determined that the individual presents no apparent risk, individuals requiring access to NATO Classified Information may be granted such access based on an Interim or Temporary PSC, issued in accordance with national laws and regulations (Supporting document on national PSC procedures and requirements (AC/35-D/1043) identifies Nations that can issue an Interim or Temporary PSC).

41. The parent NSA/DSA or other competent security authority shall ensure that the individual:

(a) have a need-to-know;

(b) have been briefed on their security obligations in respect to the protection of NATO Classified Information; and

---

8 Insider Threat is represented by personnel who have privileged access to NATO Classified Information and/or NATO assets by virtue of their role within the organization and could subsequently abuse this access to destroy, damage, remove or disclose NATO Classified Information and/or NATO assets either by intention or negligence.

9 Additional guidance on the establishment of a layered approach to addressing the management of the Insider Threat can be found in the Supporting document on Security Education and Awareness (AC/35-D/1029-REV1).

(c) have acknowledged their responsibilities either in writing or an equivalent method which ensures non-repudiation.

Provisional Appointments

42. When an individual is to be assigned to a post that requires a PSC at a level higher than they currently possess, exceptionally the assignment may be made on a provisional basis, provided that the following requirements are met:

(a) the individual possesses a current PSC;

(b) the security clearance process for obtaining the level of PSC required for the post has already been initiated; and

(c) satisfactory checks have been made by the employing NATO Civil or Military body that the individual has not seriously or repeatedly infringed security regulations.

43. The record of individuals that have been granted access in accordance with paragraphs 40 to 42 above shall be maintained by the responsible Security Office and shall be periodically forwarded to the NOS. The Head of the NATO Civil or Military body shall inform the parent NSA/DSA on granting such access to the individual.

Temporary Access

44. Exceptionally, individuals may be authorised, on a one-time basis, access to NATO information classified one level higher than their current PSC. In order to be granted this access, 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) satisfactory checks have been made by the employing NATO Civil or Military body that the individual has not seriously or repeatedly infringed security regulations;

(d) 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

(e) a record of the exception, including a description of the information to which access was authorized, shall be maintained by the responsible Security Office.

45. 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 PSC for the higher level shall be obtained and the PSC requirements of the post updated.

Use of Interpreters

46. Exceptionally, access to NATO Classified Information for the purposes of translation or interpretation by translators or interpreters from NATO or non-NATO nations who do not have an appropriate PSC for the purposes of translation or interpretation is permitted in the following case:

(a) the language to be interpreted requires a mother tongue speaker and makes the individual essential/critical with respect to the activity;

(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 COSMIC TOP SECRET in support of the mission described by the Head of

a NATO HQ Division, or NATO Civil or Military body;

(d) 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;

(e) a record of the exceptions, including a description of the facility and of the information to which access was approved, shall be maintained by the responsible Security Office and shall be periodically forwarded to the NOS;

(f) individuals have been briefed on the relevant security procedures and have acknowledged in writing that they fully understand their responsibilities and the potential consequences should there be an unauthorised disclosure, either by intent or through negligence.

Emergency Access

47. In wartime, during periods of mounting international tension, international contingency operations or in peacetime when emergency measures require it, NATO 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 PSC, 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 by the responsible Security Office.

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

ACCESS TO NATO CLASSIFIED INFORMATION BY NON-NATO CITIZENS SERVING AS INTEGRATED STAFF OF NATO NATIONS' CIVIL OR MILITARY BODIES

49. Non-NATO citizens[10] serving as integrated[11] staff of NATO Nations' civil or military body (e.g. Armed Forces, government structures) may be authorised access to NATO Classified Information provided such access is necessary in support of a specified NATO operation, mission, activity, programme. Prior to providing access to NATO Classified Information, it shall be incumbent upon the respective NATO Nation's NSA/DSA to satisfy itself and confirm as appropriate that the following conditions are met:

(a) the NATO Nation is willing to share access to its own national classified information of a similar type and classification level with the non-NATO nation of which the integrated staff member is a citizen;

(b) the individual in question has been granted a PSC based on a clearance process no less rigorous than that required for a NATO national in accordance with the NATO Security Policy and its supporting directives; noting that a PSC is not required for access to NR information;

[10] These provisions do not apply to Canadian Permanent Residents. For the purpose of this Directive they will be treated as NATO nationals.

[11] Members of non-NATO nations are considered to be integrated members of either a NATO Nation's civil or military body when they are fully incorporated into that body as constituent members therein and are treated by that body as being equal in every manner, where their PSC is either provided by their parent nation or the NATO Nation with the same legal obligations as a NATO national.

(c) the NATO Nation has sufficient control and jurisdiction over the individual in order to take appropriate legal action and hold them accountable for the improper handling of NATO Classified Information; and

(d) access is not provided to ATOMAL or other Special Category information.

50. All other cases where individuals of non-NATO nations and International Organizations require access to NATO Classified Information are detailed in C-M(2002)49 Enclosure H and its supporting directives.

Date: (DD/MM/YYYY) ___/___/_____

Optional (Reference Number): …….

REQUEST FOR PERSONNEL SECURITY CLEARANCE CONFIRMATION

1. Please confirm whether the individual listed below has a Personnel Security Clearance (PSC) to the depicted level.

Surname:
……..

Forename(s) (as shown on Passport/ID):
……..

Date of Birth (DD/MM/YYYY): ___/___/_____

Place of Birth:
……
Nationality:
……..

Passport/ID Number (Optional)
……..

Issued by: ……..

Date of issue: (DD/MM/YYYY) ___/___/_____

2. PSC required:

Tick as appropriate, one or more of the following:

[ ] COSMIC TOP SECRET…..…….. [1]
[ ] NATO SECRET……..... [1]
[ ] NATO CONFIDENTIAL……[1]

3. Reason for request[2]:

……
……
……
……

4. Requesting Organization:

……

Name of the Security Officer: ……

Phone Number:……..

Email:……

[1] Add Special Category Designator, where applicable (e.g. ATOMAL, BOHEMIA, CRYPTO)

[2] The activity requiring PSC, its timeframe/duration, any other relevant information

(*) The marking is not part of the template.

Optional (Reference Number): …….

PERSONNEL SECURITY CLEARANCE CONFIRMATION

1. Confirmation is hereby given that:

Surname:

……..

Forename(s) (as shown on Passport/ID):

……..

Date of Birth (DD/MM/YYYY): ___/___/_____

Place of Birth:…..……

Nationality: ..……

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 the level of[1]:

……

Remarks:……
……..……

2. The validity of this confirmation will expire no later than (DD/MM/YYYY)**:** ___/___/_____

3. Confirming Authority (NSA/DSA/other competent security authority):

Name:……
……..……
……...
Phone Number:……..

Email:……

Date: (DD/MM/YYYY) ___/___/_____ Signature/Stamp (if applicable)[2] ……..

1 Insert, as appropriate, one or more of the following:
COSMIC TOP SECRET
NATO SECRET
NATO CONFIDENTIAL
Add Special Category Designator, where applicable (e.g. ATOMAL, BOHEMIA, CRYPTO)

2 Supporting document on national PSC procedures and requirements (AC/35-D/1043) identifies Nations' applicability regarding Signature or Stamp.

(*) The marking is not part of the template.