Cour Pénale Internationale

International Criminal Court

Administrative Instruction
ICC/AI/2007/006

Date: 19/06/2007

ICC POLICY ON PERSONNEL SECURITY CLEARANCES

The Registrar, for the purposes of establishing a system to clear individuals for access to protectively marked information, pursuant to Presidential Directive ICC/PD/2005/001, promulgates the following:

Explanatory note to the Administrative Instruction

The Court gathers, stores, processes and disseminates information. Much of this information is sensitive in the sense that unauthorised disclosure or modification might compromise the Court, its reputation, cases, witnesses, staff, officials or other interlocutors. Such information must be protected in an adequate and consist manner.

The Security & Safety Section is, pursuant to Article 44(2) of the Rome Statute 'In the employment of staff, the Prosecutor and the Registrar shall ensure the highest standards of efficiency, competency and integrity'', authorised by the Court to conduct background checks on those who work for the Court[1]. The present A.I. sets out the policy followed by the Security and Safety Section with regards to the assessment of the eligibility of individuals for a position of confidentiality at the Court. The assessment of the eligibility of an individual for a position of confidentiality is called 'vetting' within the context of the present A.I..

The objective of vetting is to contribute to the Court's efforts to protect and enhance the probity of staff. Thus, the vetting process establishes an opinion on the risk profile of an individual that is based on the individual's behaviour and circumstances in the recent past. Vetting focuses on the following behaviour and circumstances: general criminal offences, offences against state security and unprofessional conduct.

Section 1

Definitions

1.1. AIVD - Algemene Inlichtingen en Veiligheidsdienst (Dutch General Intelligence and Security Service).

1.2. DNSA – The Dutch National Security Authority, implemented by the AIVD.

1.3. Elected Officials - For the purpose of this Administrative Instruction, the term 'Elected Officials' is herewith defined as the President, Judges, Prosecutor, Deputy Prosecutors and Registrar and Deputy Registrar of the Court.

1.4. NSA - National Security Authority.

[1] Excluding Elected Officials.

1.5. Personnel Security Clearance - The administrative decision taken by the Court, which is taken following completion of Security Screening, certifying that the named individual may be permitted access to Protectively Marked Information (PMI) provided in the event of a need to know.

1.6. PHF - Personal History Form.

1.7. PMI – Protectively Marked Information.

1.8. Opinion - A notification issued to the Court by the DNSA certifying, on the basis of Security Screening, that an individual may or may not be allowed access to a specified level of PMI.

1.9. Protectively Marked Information – Information that is deemed sensitive and has been designated as such through a protection level commensurate with the risk for the Court or the provider in the case of compromise of the information.

1.10. PSC - Personnel Security Clearance.

1.11. PSC Certificate - A written statement issued by the SSS establishing that a named individual has been security cleared and indicating the level of PMI to which that person may have access in the event of a need to know.

1.12. Security Screening – The lawfully governed investigative procedure conducted by the competent authorities of national and international jurisdictions in order to determine the vulnerabilities of an individual and provide an assurance that nothing adverse is known which would prevent the individual being granted a Personnel Security Clearance for access to PMI.

1.13. SSS – The Security & Safety Section of the Registry.

1.14. IPASS [TOP] SECRET – A level of protection, defined through Administrative Instruction ICC/AI/2006/002 "Information classification and the handling of classified information provided by States and International Organisations", that requires a positive (D)NSA Opinion.

1.15. IPASS CONFIDENTIAL – A level of protection, defined through Administrative Instruction ICC/AI/2006/002 "Information classification and the handling of classified information provided by States and International Organisations", that requires a positive (D)NSA Opinion.

Section 2

General

2.1. Access to PMI shall be in accordance with the (level of) clearance authorised through a PSC.

Note: The ICC uses only one level of clearance for its own information (information generated by the Court or provided to the Court not as a State Secret). With regards to information provided by states as a State Secret, more levels of clearances are pertinent. This is regulated by Administrative Instruction ICC/AI/2006/002

2.2. This Administrative Instruction shall apply to any individual occupying a position of confidentiality within or in relation to the Court.

2.3. All categories of staff, contractors (such as cleaners and maintenance personnel), consultants, interns, visiting professionals, persons on loan or secondment, gratis personnel or any other category of person(s) shall be regarded to occupy a position of trust.

Note: Please note that Elected Officials are exempt from personnel security clearances by virtue of the separate conditions governing their nomination and appointment to the Court.

Section 3

Personnel Security Clearance Investigation

3.1. A PSC investigation shall only be carried out with the knowledge and explicit consent of the person being investigated and then only in accordance with applicable laws and regulations of the host country.

Note: In order to be allowed to conduct vetting, the individual to be vetted must explicitly consent with his/her vetting. Explicit consent is gathered through the PHF which requires the applicant to sign-of on a statement which authorised the Court to conduct vetting. In addition, Vacancy Announcements will be amended with a general statement that informs potential applicants of the Court's authority to perform background checks and policy to do so.

3.2. Persons declining to undergo a PSC investigation shall not be provided with a PSC.

3.3. Upon the granting of a security clearance to an individual, the SSS may issue a PSC Certificate. Such PSC Certificate shall contain the name of the individual, the level of security clearance (if applicable), the NSA security clearance (if applicable), the type and level of PMI which the individual may access, the date of issue and the date of expiry of the PSC (if applicable).

Section 4

Personnel Security Clearances

4.1. Individuals that may come in contact with PMI that is generated by the Court or provided to the Court other than as a State Secret, shall be cleared for such information through a process that shall encompass:

(a) The satisfactory completion of a SSS PSC questionnaire;

(b) The validation of information and declarations contained in the applicant's PHF;

(c) The checking of local and national criminal and security records where these exist and/or comparable governmental or police records for any officially recorded indication of disloyalty or unreliability.

4.2. For Dutch citizens, the PSC investigation as set out in subsection 4.1 may include, the completion of a C-level security clearance under the Netherlands Security Investigations Act 1996, as undertaken by the DNSA.

4.3. If any of the requirements outlined in subsection 4.1 and 4.2 cannot be met, steps shall be taken to meet these requirements through other investigative means, in accordance with applicable laws and regulations.

4.4. A PSC for PMI that is generated by the Court or provided to the Court not as a State Secret may be issued if the investigation remains incomplete but no adverse traces have been reported.

4.5. Indications of potential vulnerability to pressure need not necessarily be a reason to deny security clearance to an individual if the individual's loyalty, trustworthiness and reliability are undisputed.

4.6. In the event of engagements of short duration of individuals that may come in contact with PMI that is generated by the Court or provided to the Court not as a State Secret, and where the said individual cannot be cleared through the provisions as set out in subsections 4.1 and 4.2 due to the time constraints imposed by the engagement of short duration, a provisional clearance may be issued if no adverse traces have been found or reported on the individual, by request of and under responsibility of the Head of the organizational unit for which the individual shall work.

Note: The requirements for contracting company regarding their staff are regulated through the draft A.I. Security provisions for Agreements with Third Parties".

4.7. The Opinion provided by the DNSA under the Netherlands Security Investigations Act 1996 shall be of paramount importance for the consideration of issuance of a PSC.

4.8. Subject to the discretionary approval of the SSS, individuals in the possession of a current PSC issued by a recognised NSA may elect to provide a copy of the said PSC as a means of proving their security clearance.

4.9. On the basis of a PSC issued by a recognised NSA, the SSS may choose to issue a PSC, having also considered the other information sources available to the SSS.

4.10. In the event that a positive Opinion has been given by the DNSA, but the other elements of the screening process reveal issues of potential vulnerability or evidence of poor personal integrity, the SSS shall retain discretion in the issuance of a PSC.

Section 5

Additional Clearances Requirements

5.1. Individuals that may come in contact with PMI that has been provided to the Court as a State Secret shall be cleared for such information through a process that shall comprise:

(a) The satisfactory completion of a SSS security questionnaire;

(b) The validation of information and declarations contained in the applicant's PHF;

(c) The successful completion of a clearance via the Netherlands Security Investigations Act 1996, as undertaken by the DNSA;

(d) The completion of a waiver in which the individual acknowledges to fully understand the responsibilities and the consequences if PMI was to pass into unauthorised hands.

Note: Access to State secrets demands additional control measures. The protection of State Secrets is regulated through A.I. ICC/AI/2006/002 on State Secrets.

Note: The NDSA will only provide clearances for Dutch citizens.

5.2. The DNSA clearance as set out in subsection 5.1 shall be conducted according to the DNSA standards of the:

(a) The C-level in the event of information provided as a State Secret of the level IPASS CONFIDENTIAL (or its local equivalent);

(b) The B-level in the event of information provided as a State Secret of the level IPASS SECRET (or its local equivalent);

(c) The A-level in the event of information provided as a State Secret of the level IPASS TOP SECRET (or its local equivalent).

5.3. For PMI provided to the Court as a State Secret of the level RESTRICTED, no NSA clearance is required

5.4. Individuals who consented to security screening through the DNSA at the request of the Court but were not given a positive Opinion may lodge an appeal with the DNSA.

Section 6

Responsibilities of the SSS

6.1. The SSS shall be responsible for the conduct of the PSC process.

6.2. PSC applications shall be processed via the SSS, who shall operate a 'Vetting Desk' for this purpose.

6.3. Records pertaining to a PSC shall be maintained by the SSS.

6.4. The SSS shall provide individuals with access to their PSC records upon a written request.

6.5. The SSS shall be the primary interlocutor of the Court in all dealings with the DNSA or any other NS regarding personnel security screening procedures or inquiries.

Section 7

Responsibilities of the Court

7.1. The Heads of organizational units shall identify the necessity of a PSC for each position.
Note: In practice, every position will be considered as a position of trust requiring a PSC.

7.2. The Human Resources Section shall administer the obtaining of a PSC for each position.
Note: In practice, every position will be considered as a position of trust requiring a PSC.

7.3. The Heads of organizational units shall ensure that staff requiring access to PMI have a valid PSC.

7.4. When an individual's PSC is due for revalidation, or when the position-holder changes, the Head the organizational unit in which the position is found shall ensure that the required PSC has bee sought in time.
Note: In practice, revalidation is only relevant for access to state secrets.

Section 8

Responsibilities of individual subject to PSC

8.1. Individuals subject to security screening shall apply for the PSC and provide the requeste information in a timely, efficient, intelligible and accurate manner.

8.2. Failure to provide the necessary information shall preclude the issuance of a PSC.

8.3. Any suspected fraudulent or misleading declarations or submissions discovered or revealed by a individual in the course of a security screening investigation may preclude the issuance of a PSC an shall render the individual liable for disciplinary investigation and possible disciplinary measures, i accordance with the applicable regulations of the Court.

8.4. Any suspected fraudulent or misleading declarations or submissions discovered or revealed by a applicant in the course of a security screening investigation may preclude the issuance of a PSC an shall render the applicant liable for withdrawal of an offer.

8.5. The Vetting Desk shall inform Individuals subject to security screening on the forthcoming expiry their PSC in a timely manner.

Section 9

Revalidation of a Personnel Security Clearance

9.1. An IPASS PSC shall be periodically reviewed for revalidation, at intervals not exceeding 5 years for IPASS TOP SECRET authorisation and 10 years for all other levels. The period shall be determined from the date of issue of the most recent PSC.

9.2. Investigations for the renewal of the PSC shall include the period since the previous PSC was issued.

9.3. The SSS shall the review any information arising from the course of the revalidation checks against its own records and shall then formulate an opinion as to the issuance or renewal of a PSC.

9.4. In the event of a DNSA issued security clearance, the DNSA re-validation shall be conducted in accordance of the requirements of the Netherlands security Investigations Act 1996.

9.5. Where a PSC has not been revalidated before it expires, a further period of 12 months may be allowed for the revalidation to be completed, provided that the necessary revalidation procedure has already commenced.

9.6. If, at the end of the additional 12-month period as set out in subsection 9.5, the PSC revalidation has still not been completed, the individual shall be moved to duties that do require not a PSC, i.e. duties that do not require access to the PMI.

Section 10

Adverse Information

10.1. If adverse information pertaining to any individual becomes known, the matter shall be referred to the SSS in order that a determination may be made as to whether that individual may continue to hold a PSC.

10.2. The determination as set out in subsection 10.1 shall be made in consultation with the relevant Head of Organ and the Registrar.

10.3. In the event the SSS sees reason to decline the issuance of a PSC or withdrawing a PSC, the SSS shall notify the relevant Head of Organ and the Registrar on the reasons and recommended action. In the event the individual is an applicant, the recruiting organization unit and the Head of the Human Resources Section shall be notified of the reasons and recommended action.

Section 11

Security Awareness and Briefing of Individuals

11.1. Individuals holding a PSC shall be trained annually on the security policies of the Court and their responsibility to protect and prevent PMI from falling into unauthorised hands.

Section 12

Provisional PSC appointments

12.1. When an individual that does not hold a PSC is to be assigned to a position that requires a PSC, the assignment may be made on a provisional basis, provided that:

(a) Action has been initiated to obtain the PSC;

(b) No objection has been received from or via the DNSA or other competent authority;

(c) Satisfactory checks have been made that the individual has not seriously or repeatedly infringed Court security regulations.

Note: The Court employs staff before the vetting process is finished. This provision details the conditions under which the Court can employ such uncleared individuals.

12.2. Provisional appointments shall not extend beyond six months duration, dated from the time the individual takes up the position.

12.3. Provisional appointments may be extended for another six months if security screening has been initiated and no adverse information was produced to date.

Section 13

Emergency access

13.1. In exceptional cases, the Heads of Organ may grant, in writing, access to PMI to individuals who do not possess the requisite PSC, provided such permission is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned.

13.2. The advice of the SSS shall be sought if emergency access as set out in subsection 13.1 is required.

13.3. A record of this permission describing the information to which access was given shall be maintained by the appropriate organizational unit.

Section 14

Access by non-Court personnel

14.1. Non-Court personnel may be granted access to PMI that is provided to the Court as a State Secret, on a case-by-case basis, provided that:

(a) Access is necessary in support of a specified Court programme, project, contract, operation or related task; and

(b) The individual is in possession of NSA or DNSA issued security clearance of an appropriate level; and

(c) The prior written consent of the information "owner" is obtained that specifies access to a specific bloc of PMI.

14.2. Non-Court personnel may be granted access to PMI that is generated by the Court or provided to the Court other than as a State Secret, on a case-by-case basis, provided that:

(a) Access is necessary in support of a specified Court programme, project, contract, operation or related task; or

(b) Access is a statutory right within the Court.

Note: This caters for Defence and other parties to the judicial, operational and administrative functions of the Court.

Section 15

Final Provisions

15.1. Violations of this Administrative Instruction may result in disciplinary action in accordance with the Staff Rules and Regulations, as applicable.

15.2. Staff wishing to request exceptions to any section of this policy should do so by written communication to the Safety and Security Section.

15.3. This Administrative Instruction shall be reviewed, and amended when necessary, yearly by the Information Security Officer as part of the Court's information security management process.

15.4. This Administrative Instruction shall be applied from the date of its signature.

Bruno Cathala
Registrar