

*Original*

CONFIDENTIAL

80-05-07

PERSONNEL SECURITY

T A B L E O F C O N T E N T S

	<u>PAGE</u>
1. INTRODUCTION-----	1
1.1. Purpose and Scope-----	1
1.2. Application-----	1
1.3. Authorities and Cancellations-----	1
1.4. Roles and Responsibilities-----	1
1.5. Definitions-----	3
2. CLEARANCE OF PERSONNEL-----	5
2.1. Principles and Policy-----	5
2.2. Security Clearances-----	7
2.2.1. Appointments to New or Vacant Positions----	7
2.2.2. Denial of Security Clearance During the Appointment Process-----	9
2.2.3. Revocation of Security Clearance-----	9
2.2.4. Exceptional Cases-----	10
2.3. Reliability Clearances-----	11
2.3.1. Appointments to New or Vacant Positions----	11
2.3.2. Denial of Reliability Clearance During the Appointment Process-----	13
2.3.3. Revocation of Reliability Clearance-----	13
2.4. Documentation Relating to the Granting of Clearances	13
2.5. Updating of Clearance Documentation-----	14
2.6. Review of Clearance Requirements-----	14
2.7. Reciprocal Acceptance of Clearances-----	15
2.8. Termination of Clearances-----	15
3. IDENTIFICATION OF PERSONNEL-----	15
4. SECURITY EDUCATION AND AWARENESS-----	16
4.1. Security Education Program-----	16
4.2. Acknowledgement of Security Responsibilities-----	17
4.3. Refresher Briefings-----	17
4.4. Foreign Travel Briefings-----	17
5. PERSONNEL SECURITY CONTROL-----	17
6. PRIVATE SECTOR PERSONNEL SECURITY-----	18
6.1. Responsibility-----	18
6.2. Clearance of Personnel-----	18
6.3. Identification of Personnel-----	19
6.4. Security Education Program-----	19
6.5. Acknowledgement of Security Responsibilities-----	19
Annex A - Security Clearance Questionnaire-----	
Annex B - Criteria for Granting Security Clearances-----	

CONFIDENTIAL

1. INTRODUCTION

1.1. Purpose and Scope

1.1.1. In order to ensure that comprehensive and consistent protection is provided for the classified information and material assets of the Government of Canada, the security programs of departments and agencies must recognize six essential elements:

- a) administration of security;
- b) personnel security;
- c) physical security;
- d) communications-electronic security;
- e) electronic data processing security, and
- f) technical security.

The second of these program elements, personnel security, involves the development and implementation of policy and procedures related to the suitability, identification and security awareness of personnel who are to have access to classified information and material assets.

1.1.2. This chapter provides directives and guidelines to be followed by departments and agencies in:

- a) clearing government and non-government personnel for access to classified information and material assets;
- b) providing identification documents to personnel;
- c) developing security education and awareness programs, and
- d) applying personnel security controls.

1.2. Application

1.2.1. This chapter applies to departments and ministries of state and other government institutions listed in Annex A of A Policy for the Protection of Government of Canada Assets.

1.3. Authorities and Cancellations

1.3.1. This chapter is issued under the authority of a Cabinet Decision by which the Treasury Board is required to approve and issue directives and guidelines for departments and agencies concerning the six elements of security outlined in 1.1.1. above.

1.3.2. This chapter cancels Cabinet Directive No. 35 dated 63-12-18.

1.4. Roles and Responsibilities

1.4.1. This section identifies the most important inter-relationships and responsibilities of those components of the Government of Canada specifically concerned with personnel security.

.../2

007283

- 1.4.1.1. The departmental security officer, designated by and under the direction of the deputy head, is responsible for the development and implementation of the departmental security program which shall include the implementation of the security and reliability clearance requirements, and the conducting of a personnel security education program;
- 1.4.1.2. Deputy heads, under the direction of Ministers, shall be responsible for all aspects of personnel security in their respective departments or agencies, and for ensuring compliance with personnel security policy, directives and guidelines;
- 1.4.1.3. The supervisor is responsible for reviewing the duties of a vacant position and identifying situations where classified assets require protection. Based upon the needs as reflected in the position description, the supervisor will prepare or assist in the preparation of a statement of qualifications for use in staffing;
- 1.4.1.4. The Security Review Board of Inquiry, composed of three deputy heads, shall conduct an inquiry in a manner consistent with the Public Service Security Inquiry Regulations. The board shall hear the employee, with counsel if desired, and shall recommend to the Governor-in-Council either support or rejection of the original decision of the deputy head;
- 1.4.1.5. The selection board, in the case of a vacant position with a security or reliability clearance requirement, shall assess the candidates taking into account all basic requirements except the security or reliability clearance. Based on this assessment, the board shall identify the highest ranking candidates. In the case of a vacant position with a requirement for a reliability clearance, the selection board, based on the results of the inquiries and checks required for the clearance, shall also decide on the suitability of a candidate for reliability clearance and shall publish an eligible list;
- 1.4.1.6. The Department of National Defence (DND) and the Canadian Forces are responsible for conducting security clearance investigations for members of the Canadian Forces and persons employed by DND;
- 1.4.1.7. The Department of Supply and Services is responsible for arranging for the clearance of persons who are contracted to provide goods or services to the government and who are to have access to classified information or material assets. It is also responsible for ensuring the adequacy of personnel security measures for the protection of classified information and material assets provided under contract to private sector facilities or to persons outside the government;

.../3

007284

- 1.4.1.8. The Public Service Commission of Canada is responsible for providing direction regarding appointments made under the Public Service Employment Act to positions requiring security or reliability clearances. It is also responsible for assisting in the provision of personnel security training programs for employees;
- 1.4.1.9. The Royal Canadian Mounted Police (R.C.M.P.), except as otherwise provided, is responsible for:
- i) providing advice and assistance to departments and agencies on the implementation of the personnel security directives and guidelines,
  - ii) auditing the implementation of personnel security policy, directives and guidelines by departments and agencies, and
  - iii) assisting departments and agencies in determining the suitability of persons for security and reliability clearances by, where required, checking criminal and subversive records, conducting field investigations, and providing comments on the significance of the information provided relevant to the granting or withholding of security clearances;
- 1.4.1.10. The Treasury Board, supported by the Treasury Board Secretariat, is responsible for approving and issuing the personnel security directives and guidelines and monitoring their implementation and effectiveness.

1.5. Definitions

- 1.5.1. "asset" means any information or material asset owned or in the custody of the Government of Canada;
- 1.5.2. "candidate" means one who seeks, or is nominated for a vacant position within the Government of Canada;
- 1.5.3. "classified" means assigned a designation of Top Secret, Secret, Confidential, or Protected;
- 1.5.4. "consent form" means the form, to be signed by a person who requires a security or reliability clearance, which gives consent for inquiries concerning this person, to be undertaken;
- 1.5.5. "departmental security officer" means the senior official who is appointed by the deputy head to be responsible for the development and implementation of the departmental security program;
- 1.5.6. "deputy head" means
- i) within a department named in Schedule A to the Financial Administration Act, the deputy minister of that department,
  - ii) within the Canadian Forces, the Chief of Defence Staff,
  - iii) within the Royal Canadian Mounted Police, the Commissioner, and

- iv) within any other department or agency, the chief executive officer thereof or, if there is no chief executive officer, such person as the Governor-in-Council may designate as the deputy head;
- 1.5.7. "eligible list" means one or more lists of the highest ranking candidates in a competition as the Public Service Commission, department or agency, considers necessary to provide for the filling of a vacancy or anticipated vacancy;
- 1.5.8. "employee" means an officer or employee of the Government of Canada;
- 1.5.9. "encumbered position" means a position to which an employee has been appointed;
- 1.5.10. "field investigation" means inquiries conducted to assist departments and agencies in determining the suitability of a person for a security clearance;
- 1.5.11. "government" means the Government of Canada;
- 1.5.12. "position description" means the written explanation of the functions, objectives, job complexity and accountability of a position. It also includes a description of the essential and desirable qualifications.
- 1.5.13. "reliability clearance" means the authorization in writing by a deputy head, or a security officer acting on the deputy head's behalf, for a person to have access to information or material assets designated as PROTECTED;
- 1.5.14. "security clearance" means the authorization in writing by a deputy head, or a security officer acting on the deputy head's behalf, for a person to have access to information or material assets designated as TOP SECRET, SECRET or CONFIDENTIAL;
- 1.5.15. "security clearance questionnaire" means the form which must be completed by a candidate prior to the screening for a security clearance. It must contain adequate and reliable background information covering the previous 10 years;
- 1.5.16. "selection board" means the person or persons who assess and rank candidates in terms of their qualifications for appointment;
- 1.5.17. "statement of qualifications" means a written specification of the essential and desirable qualifications pertinent to the staffing of a position or group of positions, and
- 1.5.18. "subversive or hostile activities" means
- i) espionage or sabotage,
  - ii) activities of any person or group of persons directed toward the commission of terrorist acts in or against Canada or other states,

.../5

- iii) activities directed toward accomplishing governmental change within Canada or other states by the use of or the encouragement of the use of force, violence or any criminal means,
- iv) activities directed toward gathering intelligence relating to Canada or any state allied or associated with Canada, and
- v) activities directed toward threatening the safety of Canadians, employees of the Government of Canada or property of the Government of Canada.

2. CLEARANCE OF PERSONNEL

2.1. Principles and Policy

2.1.1. The Government of Canada has a responsibility to ensure the suitability of all persons who are to have access to classified information and material assets. The directives and guidelines in this chapter were developed in accordance with the following principles:

- 2.1.1.1. The deputy head is responsible for the administration of policy and procedures related to the clearance of personnel within the department or agency.
- 2.1.1.2. Clearance shall be required of persons only when the clearance is related to their duties and responsibilities.
- 2.1.1.3. In the clearance process, every effort must be made to safeguard the interests of the person concerned.
- 2.1.1.4. The ultimate determination of whether the granting of a clearance is consistent with the interests of the nation and the government must conform with the provisions of this chapter and be based on all available information. Where reasonable doubt exists, the interests of the nation must take precedence.
- 2.1.1.5. When a person is to be denied a job opportunity for reasons of clearance, he/she is entitled to be informed of the basis for this judgment and provided an opportunity to refute the validity of the evidence before an independent board. In all cases, however, this principle must be balanced by the necessity to protect the confidentiality of sources and information.
- 2.1.1.6. The clearance process is to be administered in a manner which minimizes unnecessary expense or delay.
- 2.1.1.7. The clearance process is not to be viewed as replacing the need for management to monitor on an ongoing basis the suitability of personnel for access to classified information and material assets.

2.1.2. The following operational policy regarding the clearance of personnel was approved by the Cabinet on

- 2.1.2.1. A security clearance shall be a mandatory requirement for all persons who are to have access to information and material assets designated as TOP SECRET, SECRET, or CONFIDENTIAL. Screening for a security clearance shall include verification of the person's identification, educational qualifications, employment record, references and credit rating, and a check of criminal records based on the security clearance questionnaire. In addition, a field investigation shall be conducted for all TOP SECRET clearances and for SECRET clearances if deemed necessary by the investigative agency.

*Handwritten notes:*  
2.1.1.5. 3.1.1.1.1.?  
2.1.1.6. 2.1.1.6.1.?  
2.1.1.7. 2.1.1.7.1.?  
2.1.2.1. 2.1.2.1.1.?

- 2.1.2.2. A reliability clearance shall be mandatory requirement for all persons who are to have access to information and material assets designated as PROTECTED. Screening for a reliability clearance shall include verification of the person's identification, educational qualifications, employment record and references. In addition, credit rating and criminal records checks based on fingerprints shall be undertaken, if these requirements are specified in the statement of qualifications or in a contract or agreement.
  - 2.1.2.3. The requirements for access to classified information or material assets shall be specified in position descriptions for employees of the government and in contracts or agreements with persons or organizations outside the government.
  - 2.1.2.4. In addition to a security or reliability clearance, a person must have a need for access to any classified information or material assets in connection with the performance of official duties or contractual obligations, before such access is granted.
  - 2.1.2.5. Responsibility for the verification of the identification, educational qualifications, employment record, references and, where required, the credit rating of persons for employment within the government rests with the employing department or agency. In cases where the procurement of goods or services from the private sector is contracted by a department or agency, the responsibility rests with the Security Branch (Supply Administration) of the Department of Supply and Services. The assistance of the Royal Canadian Mounted Police shall be requested in conducting security clearances and reliability clearances, as specified in 2.2.1.11. and 2.2.1.12.
  - 2.1.2.6. Any decision made to deny, revoke or suspend a security or reliability clearance shall be reported in writing to the person concerned and to the supervisor concerned.
  - 2.1.2.7. Departments and agencies shall comply with the procedures established for the independent review and redress of a decision made to deny, revoke, suspend or reduce the security or reliability clearance of a government employee. These procedures shall be specified in the directives and guidelines issued pursuant to this operational policy. In this regard, members of the Canadian Forces and members of the Royal Canadian Mounted Police are subject to the procedures in the Queen's Regulations and Orders for the Canadian Forces and the Royal Canadian Mounted Police Act, respectively. Employees of departments and agencies, which are not subject to the Public Service Employment Act or Public Service Staff Relations Act, will be provided an independent review through the establishment of a Board of Inquiry appointed pursuant to the Inquiries Act.
- 2.1.3. Through an ongoing security education program, persons who have been granted security clearances or reliability clearances shall be initially advised of their security duties, responsibilities and liabilities, and subsequently reminded.

.../7

007288

2.2. Security Clearances

2.2.1. Appointments to New or Vacant Positions

- 2.2.1.1. Each time a position is created or becomes vacant, the supervisor shall review the duties associated with the position to determine if there is a requirement for access to assets classified in the national interest.
- 2.2.1.2. If a position involves a requirement for access to information and/or material assets classified in the national interest, this requirement shall be specified in the position description. For example, the following statement could appear:
- "This position involves access to information and/or material assets designated as TOP SECRET".*
- 2.2.1.3. If a position involves access to information and/or material assets classified in the national interest, the requirement for a security clearance shall be included as a basic requirement in the statement of qualifications. For example the following statement could appear:
- "The candidate must be able to be cleared to TOP SECRET".*
- 2.2.1.4. In the case of a position with a security clearance requirement, the selection board shall assess the candidates, taking into account all basic requirements except security clearance. Based on this assessment, the board shall identify the highest ranking candidates.
- 2.2.1.5. Based on departmental staffing requirements and time constraints, security clearance checks and investigations shall be conducted for some or all of the highest ranking candidates, and may be conducted before or after publication of the eligible list.
- 2.2.1.6. If an eligible list is published before candidates are security cleared, the list shall specify that appointment is contingent on the granting of a security clearance.
- 2.2.1.7. Those candidates who are to be security cleared shall be informed of:
- a) the reasons for seeking background information;
  - b) the type of checks and investigations to be conducted, and
  - c) the ramifications of concealing information which may affect the granting of a clearance.
- 2.2.1.8. Those candidates who are to be security cleared shall be requested, where appropriate, to provide:
- a) documents related to identification, education and employment;
  - b) letters of reference;
  - c) completed security clearance questionnaire (see Annex A);
  - d) authorization for a credit rating check;
  - e) fingerprints, and
  - f) a completed consent form.

- 2.2.1.9. Candidates who refuse to provide the documentation specified in 2.2.1.8. shall be ineligible for appointment to the position.
- 2.2.1.10. Candidates who are to be security cleared must be able to provide adequate and verifiable background information on the security clearance questionnaire covering the previous 10 years.
- 2.2.1.11. In the case of candidates who are to be security cleared to the level of Top Secret, the department or agency shall:
- a) verify, to the extent necessary to establish the bona fides and suitability of the candidates, the identification, educational qualifications, employment record, credit rating and character references of the candidates for the previous 10 years, and
  - b) when possible and practical, conduct a preliminary security interview to determine if there is anything in the candidate's background which may be relevant to his security status or could preclude the issuance of a Top Secret security clearance. The result of the interview should be made available to the RCMP, together with particulars of three of the candidate's closest associates excluding character references named in the security clearance questionnaire.
  - c) submit the candidate's fingerprints and completed security clearance questionnaire to the RCMP with requests for criminal and subversive records checks and field investigations.
- 2.2.1.12. In the case of candidates who are to be security cleared to the level of Confidential or Secret, the department or agency shall:
- a) verify, to the extent necessary to establish the bona fides and suitability of the candidates, the identification, educational qualifications, employment record, credit rating and character references of the candidates for the previous 10 years, and
  - b) submit the candidates' fingerprints and completed security clearance questionnaires to the R.C.M.P. with requests for criminal and subversive records checks.
- 2.2.1.13. The RCMP is responsible for conducting criminal and subversive records checks for all security clearances and for conducting field investigations for all TOP SECRET clearances and for SECRET clearances, if deemed necessary by the RCMP (see 2.2.1.14). The RCMP will inform departments and agencies of the results of its investigations and checks including, where appropriate, comments on the significance of the information relevant to the granting or withholding of the security clearance.
- 2.2.1.14. The Department of National Defence (DND) is responsible for conducting security clearance field investigations for members of the Canadian Forces and persons employed by DND.

2.2.1.15. Based on the results of the checks and inquiries specified in 2.2.1.11 and 2.2.1.12., the deputy head shall decide on the suitability of a candidate for security clearance. The criteria for granting a security clearance are in Annex B.

2.2.2. Denial of Security Clearance During the Appointment Process

2.2.2.1. If doubt arises regarding the suitability of a candidate for security clearance, the departmental security officer, or person designated by the deputy head for this purpose, shall consult with the RCMP or other source of the information which raised the doubt and then shall interview the candidate, regardless of whether he/she is an employee. At this interview, the candidate shall be informed of the reasons for doubt, to the fullest extent possible without jeopardizing the national interest or sources of information, and given an opportunity to resolve the doubt.

2.2.2.2. *After interviewing the candidate, the departmental security officer, or person designated by the deputy head for this purpose, may conduct further inquiries to help resolve the doubt and may request further assistance from the RCMP.*

2.2.2.3. Based on all information available, a report shall be submitted to the deputy head for decision. The decision of the deputy head shall be submitted to the candidate in writing.

2.2.2.4. If the deputy head decides during an appointment process that an employee is unsuitable for security clearance, the employee may request, within 14 days of notification of the decision, that the Minister recommend to the Governor-in-Council that a Security Review Board of Inquiry be established.

2.2.2.5. The Security Review Board of Inquiry, composed of three deputy heads, shall conduct an inquiry in a manner consistent with the Public Service Security Inquiry Regulations. The board shall hear the employee, with counsel if desired, and shall recommend to the Governor-in-Council either support or rejection of the original decision of the deputy head.

2.2.2.6. Where an employee is denied a security clearance in the process of applying for a new or vacant position, the deputy head shall decide if the employee can be permitted to remain in his/her current position. Directives 2.2.3.5. and 2.2.3.6. will apply, as appropriate.

2.2.3. Revocation of Security Clearance

2.2.3.1. If doubt arises regarding the suitability of an employee already granted a security clearance, the department or agency shall take any interim measures which are necessary to ensure the security of information and material assets classified in the national interest to which the employee may have access. Such interim measures may include removing the classified assets or, where necessary, suspending the employee from his duties with pay.

.../10

2.2.3.2. The departmental security officer, or person designated by the deputy head for this purpose, shall review the information which raised the doubt and shall then interview the employee. At this interview, the employee shall be informed of the reasons for doubt to the fullest extent possible without jeopardizing the national interest or sources of information, and shall be given an opportunity to resolve the doubt.

2.2.3.3. After interviewing the employee, the departmental security officer, or person designated by the deputy head for this purpose, may conduct further inquiries to help resolve the doubt and may request further assistance from the RCMP.

2.2.3.4. Based on all information available, a report shall be submitted to the deputy head for decision. The decision of the deputy head shall be submitted to the employee in writing and shall contain notification of any other rights respecting review or redress.

2.2.3.5. Where the decision is to revoke the security clearance of an employee, the deputy head shall decide:

- a) whether the employee might be safely and usefully appointed to a less sensitive position in the department or agency or elsewhere in the public service, the reasons having been explained to the employee to the fullest extent possible, or
- b) if appointment elsewhere is not possible, whether the employee should be provided the opportunity to resign from the public service, or
- c) if the employee does not resign, whether a proposal should be made to dismiss the employee from the public service.

2.2.3.6. If the deputy head recommends the dismissal of the employee, an inquiry shall be conducted in accordance with the Public Service Security Inquiry Regulations made pursuant to subsection 7(7) of the Financial Administration Act. For those agencies which are not subject to Section 7(7) of the Financial Administration Act, such inquiries shall be conducted by a Board of Inquiry appointed by the Governor-in-Council pursuant to the Inquiries Act.

2.2.4. Exceptional Cases

2.2.4.1. Before a Minister makes a recommendation for an Order-in-Council appointment which requires access to classified assets, he/she must ensure that a nomination does not go forward until the following security measures are taken on their behalf and confirmed by their departmental security officer.

- a) At an early stage, before any commitment is made, a "cursory records check" should be done. For this purpose, the departmental security officer requires:
  - i) full name of the candidate/s;
  - ii) date and place of birth (if the actual birth date is not readily available, approximate age should be given. Regarding "place of birth", it is important to know whether of Canadian or foreign birth. In the latter case, country of origin and date of landing should be given);
  - iii) current or immediate past employment and location, and
  - iv) current address.
- b) This check can be done within a few hours. If an adverse trace is revealed, additional information and time may be required to confirm whether the trace is relevant or not. The Minister shall be informed promptly by the departmental security officer of the extent of the risk factor, if applicable.

*This should not be in a public statement*

- c) Following a satisfactory records check, the candidate/s shall be informed of the security clearance requirement and the departmental security officer shall be directed to arrange for the completion of the security clearance questionnaire and fingerprint form.
- d) The completed forms shall be dispatched "by hand" to the RCMP for a priority comprehensive check of records.
- e) The above process can be completed within a day or two and provides the basis for a CONFIDENTIAL or SECRET clearance. A TOP SECRET clearance will require a field investigation which may take several days or weeks.
- f) If a risk factor is identified at any stage of the above process, the Minister shall be informed promptly by the departmental security officer of the facts and/or allegations.
- g) A statement confirming a satisfactory security screening or clearance process shall be included in the covering note of the Minister's nomination.
- h) In cases where senior government employees are to be appointed to Boards, Councils, and other agencies while in status, a note shall be included to confirm their current departmental security clearance status.

2.2.4.2. In certain exceptional cases, the deputy head may decide to grant a security clearance to a person about whom adequate and verifiable background information cannot be obtained. In these instances, there must be strong, positive evidence of the person's trustworthiness, and the deputy head must decide that the value of the person's services justifies the risk involved.

2.2.4.3. In certain extreme emergency situations, the deputy head may decide to grant a security clearance to a person, although time constraints do not permit completion of all checks and inquiries. In these instances, it must be determined that the exceptional circumstances causing the emergency are of such a nature that the delay caused by awaiting clearance would be harmful to the national interest.

2.2.4.4. Departments and agencies shall annually report to the Treasury Board the names of persons who were granted a security clearance under the circumstances mentioned in 2.2.4.2. - 2.2.4.3. above, and the special circumstances related to the granting of these clearances.

### 2.3. Reliability Clearances

#### 2.3.1. Appointments to New or Vacant Positions

2.3.1.1. Each time a position is created or becomes vacant, the supervisor shall review the duties associated with the position to determine if there is a requirement for access to information and/or material assets classified in the public interest.

2.3.1.2. If a position involves a requirement for access to information and/or material assets classified in the public interest, this requirement shall be specified in the position description. For example, the following statement could appear:

*"This position involves access to information and/or material assets designated as PROTECTED".*

2.3.1.3. If a position involves access to information and/or material assets classified in the public interest, the requirement for a reliability clearance shall be included as a basic requirement in the statement of qualifications. For example, the following statement could appear:

*"The candidate must be able to be cleared for access to PROTECTED assets. The reliability clearance will include a credit rating check and a criminal records check based on fingerprints".*

007293

- 2.3.1.4. In the case of a position with a reliability clearance requirement, the selection board shall assess the candidates, taking into account all basic requirements except reliability clearance. Based on this assessment, the highest ranking candidates shall be identified.
- 2.3.1.5. Prior to publishing an eligible list, reliability clearance checks and inquiries shall be conducted on all candidates to be placed on the list.
- 2.3.1.6. Those candidates who are to be cleared for reliability shall be requested, where appropriate, to provide:
  - a) documents related to identification, education and employment;
  - b) letters of reference;
  - c) authorization for credit rating check, if specified as a basic requirement;
  - d) fingerprints, if specified as a basic requirement, and
  - e) a completed consent form.
- 2.3.1.7. Candidates who refuse to provide the documentation specified in 2.3.1.6. shall be ineligible for appointment to the position.
- 2.3.1.8. In the case of candidates who are to be cleared for access to PROTECTED assets, the department or agency shall:
  - a) verify, to the extent necessary to establish the bona fides and suitability of the candidates, the identification, educational qualifications, employment record and character references of the candidates;
  - b) if specified as a basic requirement, submit the candidates' names for a credit rating check, and
  - c) if specified as a basic requirement, submit the candidates' fingerprints to the RCMP, with requests for criminal records checks.
- 2.3.1.9. The RCMP is responsible for conducting criminal records checks for reliability clearances, if such checks are specified as a basic requirement.
- 2.3.1.10. Based on the results of the inquiries and checks specified in 2.3.1.8., the selection board shall decide on the suitability of a candidate for reliability clearance and shall publish an eligible list.

.../13

2.3.2. Denial of Reliability Clearance During the Appointment Process

2.3.2.1. A candidate who is considered by the selection board to be unsuitable for reliability clearance shall be judged to be unqualified for the position and will be so notified in writing. *The unsuccessful candidate has a right of appeal as provided for in Section 21 of the Public Service Employment Act or as otherwise provided for in Section 2.1.2.7. above.*

2.3.3. Revocation of Reliability Clearance

2.3.3.1. If doubt arises regarding the reliability of an employee already granted a reliability clearance, the department or agency shall take any interim measures which are necessary to ensure the security of information and material assets classified in the public interest to which the employee may have access.

2.3.3.2. The departmental security officer, or the person designated by the deputy head for this purpose, shall review the information which raised the doubt and shall then interview the employee. At this interview, the employee shall be informed of the reasons for doubt, to the fullest extent possible without jeopardizing sources of information, and shall be given an opportunity to resolve this doubt.

2.3.3.3. *After interviewing the employee, the departmental security officer, or the person designated by the deputy head for this purpose, may conduct further inquiries to help resolve the doubt and may request assistance from the RCMP.*

2.3.3.4. Based on all information available, a report shall be submitted to the deputy head for decision. The decision of the deputy head shall be submitted to the employee in writing.

2.3.3.5. Where the decision is to revoke the reliability clearance of an employee, the deputy head will decide to transfer, release, demote or dismiss the employee in accordance with the applicable legislation.

2.4. Documentation Relating to the Granting of Clearances

2.4.1. The granting of security or reliability clearances shall be made a matter of record and made a permanent part of the employee's personnel file or other appropriate record. Records shall reflect the date and type of checks, inquiries and investigations conducted, the date clearance was granted, and the name and position of the person who granted the clearance.

.../14

- 2.4.2. Information obtained for purposes of reliability and security clearances:
- a) shall be assigned the appropriate security designation;
  - b) shall, subject to the provisions of the Freedom of Information and Privacy Acts, be made available only to the deputy head, the departmental security officer or persons designated by them;
  - c) shall be administered in such a way that its personal and private character is maintained;
  - d) if it raises doubt about the person's loyalty or reliability, shall be returned to the RCMP for review in the case of a person concerned who is to be employed in another department, or for disposal in the case of termination of employment;
  - e) if it raises no doubt about the person's loyalty or reliability, shall be provided to the department in which the person concerned is to be employed.

2.4.3. Classified information obtained for purposes of security and reliability clearances, which is considered to be additional to information normally compiled for the staffing process, shall not be placed on the personnel file of the person concerned.

2.5. Updating of Clearance Documentation

- 2.5.1. An employee who has been granted a security clearance shall update his/her security clearance questionnaire every five years. The department or agency shall submit any updated information to the RCMP, with requests for criminal and subversive records checks and investigations.
- 2.5.2. In the case of an employee with a reliability clearance which included a criminal records check as a basic requirement, the department or agency shall request an updated criminal records check from the RCMP every five years.
- 2.5.3. If a candidate is to be offered appointment to a new or vacant position more than three months after publication of the eligible list, the results of the initial inquiries and checks shall be reviewed and updated, as appropriate, for reliability clearances not requiring a criminal records check. For reliability checks which require a criminal records check and for all security clearances, updated checks shall be requested from the RCMP.

2.6. Review of Clearance Requirements *? at what level?*

- 2.6.1. Supervisors shall annually review the clearance requirements of encumbered positions to confirm that the requirements for access to classified information and/or material assets have not changed. (See 2.8.2. below)
- 2.6.2. If the duties of an encumbered position change to the extent that the clearance requirement is lowered, the clearance of the incumbent shall be modified accordingly and the incumbent shall be verbally advised of the modification.
- 2.6.3. The deputy head must approve any changes in the duties of an encumbered position, which would entail raising the clearance requirement. If the deputy head approves such changes, the appropriate checks and investigations on the incumbent shall be initiated immediately and the department or agency shall take any interim measures which are necessary to maintain the security of classified information and material assets to which the incumbent may have access.

.../15

007296

2.6.4. If the incumbent does not receive the appropriate clearance, or is unwilling to provide the necessary documentation, the deputy head shall take the appropriate administrative action.

2.7. Reciprocal Acceptance of Clearances

2.7.1. If an employee of one department or agency is transferred or appointed to a position with an identical clearance requirement in another department or agency, the receiving department or agency may accept the previous clearance of the employee.

2.7.2. The receiving department or agency shall have the right to review the information on which the original clearance was granted and may make additional inquiries or request updated information before accepting the clearance.

2.7.3. A previous clearance shall not be accepted if it was terminated and the employee was subject to the provisions mentioned in section 5.3. below.

2.7.4. The deputy head or delegate must record the circumstances upon which a decision to deny a previous clearance was based.

*of course  
it has  
for 72  
memo  
for clearance  
than this*

2.8. Termination of Clearances

2.8.1. The security clearance or reliability clearance of an employee shall terminate when the employee ceases to be employed.

2.8.2. If the duties of an encumbered position change to the extent that the need-to-know clearance requirement no longer exists, the clearance of the incumbent shall be terminated and the incumbent shall be verbally advised of the termination. (See 5.3. below)

3. IDENTIFICATION OF PERSONNEL

3.1. Identification cards shall serve only to establish identity and the holder's association with a department, agency or a private employer, but shall convey no entitlement for access.

3.2. The departmental security officer, or the person designated by the deputy head for this purpose, shall arrange the issue of approved identification cards to all employees who have access to classified information and material assets.

3.3. An approved identification card shall contain at least the following:

- a) name of card holder;
- b) name of employer;
- c) "head-and-shoulders" photograph of card holder;
- d) signature of card holder;
- e) signature of authorizing authority;
- f) date of card issue;
- g) card serial number, and
- h) expiry date.

3.4. The departmental security officer, or the person designated by the deputy head for this purpose, shall issue approved temporary identification cards, pending the issue of permanent identification cards, or for personnel whose term of employment does not warrant permanent identification cards.

*Redundant*

- 3.5. An approved temporary identification card shall contain:
- a) name of card holder;
  - b) name of employer;
  - c) physical description of card holder (height, weight, eye color, hair color and complexion);
  - d) signature of card holder;
  - e) signature of authorizing authority;
  - f) date of issue;
  - g) date of expiry, and
  - h) card serial number.
- 3.6. The departmental security officer shall establish procedures for the regular review and update of identification cards.
- 3.7. The departmental security officer shall ensure inventory control and security of identification card stock are in accordance with the highest designation associated with the area in which the cards are to be used.

4. SECURITY EDUCATION AND AWARENESS

4.1. Security Education Program

4.1.1. The departmental security officer shall establish an appropriate security education program for all departmental employees who have a security or reliability clearance. *This program should stress the objectives of classifying fewer assets, declassifying more assets, and improving the protection of those assets which require safeguarding. The program should also emphasize the balance between the need to release government information to the public and the requirement for the government to protect the national interest and the public interest.*

4.1.2. The security education program shall, where appropriate, be designed to:

- a) advise employees of the adverse effects that could result from the unauthorized disclosure, destruction, modification, removal or interruption of classified information and material assets;
- b) advise employees of their personal and legal responsibility to protect classified information and material assets within their knowledge, possession or control;
- c) indoctrinate employees in the principles, criteria and procedures for the classifying, downgrading, declassifying, marking and dissemination of classified information and material assets, and alert them to the strict prohibitions on the improper use and abuse of the classification system;
- d) inform employees of the techniques employed by foreign intelligence organizations in attempting to obtain government information, and of their responsibility to report such attempts;
- e) advise employees of the penalties for engaging in subversive or hostile activities.

.../17

- f) advise employees of the strict prohibition against discussing classified information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;
- g) inform employees of the penalties for willful violation or disregard of the provisions of the security policy approved by Cabinet or these directives, and
- h) instruct employees that individuals having knowledge, possession or control of classified information and material assets must determine, prior to disseminating such assets, that the prospective recipient has the appropriate clearance, needs the asset in order to perform official government duties, and can properly protect the asset.

4.2. Acknowledgement of Security Responsibilities

- 4.2.1. The departmental security officer shall ensure all employees read and sign the Oath of Allegiance and the Oath of Office and Secrecy, using Canadian Government Specifications Board (CGSB) Standard Form 29a, before they are given access to information and material assets classified in the national interest.
- 4.2.2. The departmental security officer shall ensure that, before persons are given access to information and material assets classified in the national interest, they sign a declaration indicating that their attention has been drawn to the provisions of the Official Secrets Act.

4.3. Refresher Briefings

- 4.3.1. The departmental security officer shall establish programs to provide periodic security training for personnel having continued access to classified information and material assets. The elements outlined in 4.1.2. shall be tailored to fit the needs of experienced employees.

4.4. Foreign Travel Briefings

- 4.4.1. Employees who have had access to classified information and material assets, shall be given a briefing prior to foreign travel, to alert them of their possible exploitation under the following conditions:
  - a) travel to or through Communist-controlled countries, or
  - b) attendance at international scientific, technical engineering or other professional meetings in Canada or in any country outside Canada where it can be anticipated that representatives of Communist-controlled countries will participate or be in attendance.
- 4.4.2. Individuals who frequently travel, or attend or host meetings of the types described in 4.4.1. need not be briefed for each such occasion, but shall be initially provided with a thorough briefing and subsequently given a general reminder of security responsibilities at least annually.

5. PERSONNEL SECURITY CONTROL

- 5.1. The departmental security officer shall ensure that a record is maintained of security-related items issued to each person who has access to classified information and material assets.
- 5.2. The departmental security officer shall establish a system of control and monitoring for the issue, custody and use of all security-related items in the department or agency.

*Redacted*

*E.A. Should be touched about this in a public document.*

5.3. The departmental security officer shall establish the following procedures to be implemented when it becomes known that the employment of an individual is to be terminated or when the duties of an encumbered position change to the extent that the clearance requirement no longer exists:

- a) the debriefing of the individual on continuing security responsibilities (e.g. Official Secrets Act and departmental regulations and statutes),
- b) the revocation of access privileges to restricted areas and classified assets,
- c) the retrieval of security-related items, and
- d) the signing of a termination certificate which states that the individual's clearance has been terminated.

5.4. The departmental security officer shall establish procedures to review all access privileges of an employee who is transferred from one position to another.

6. PRIVATE SECTOR PERSONNEL SECURITY

6.1. Responsibility

6.1.1. The Security Branch (Supply Administration) of the Department of Supply and Services (DSS) is responsible for ensuring the adequacy of personnel security measures for the protection of classified information and material assets provided under contract to private sector facilities or to persons outside the government.

6.2. Clearance of Personnel

6.2.1. A department or agency intending to enter into a contract or agreement with an individual or firm in the private sector, if the contract or agreement is to involve access to classified assets, shall seek the assistance of the Security Branch (Supply Administration) of the DSS. The department or agency shall specify the clearance requirements for the private sector personnel, and these requirements shall correspond to the highest designation of assets to which the personnel may have access under the agreement. Private sector personnel requiring clearance shall include:

- a) management and key officials of the contractor,
- b) employees of the contractor, and
- c) persons under the control of, but not employed by, the contractor.

6.2.2. A department or agency entering into a contract or agreement with an individual or firm in the private sector shall specify in the contract or agreement that all private sector personnel, as in 6.2.1. above, must obtain the required clearance before access to classified assets is granted. The contract or agreement shall also specify that the Security Branch (Supply Administration) of DSS is responsible for granting the security or reliability clearances for private sector personnel, when such clearances are required contractually, and that it shall initiate all procedures required in this regard.

6.2.3. The agreement between a department or agency and an individual or firm in the private sector shall also specify that in cases where the reliability or loyalty of a person is in doubt, the employer shall co-operate with the DSS to ensure that the procedures mentioned in 6.2.4.-6.2.7. below are complied with.

6.2.4. Where the reliability or loyalty of a person referred to in 6.2.1.-6.2.3. above is in doubt, the DSS, in consultation with the employer, shall attempt to resolve the doubt. The DSS shall consult with the RCMP, or other source of the information which raised the doubt, and shall then interview

*So this all consistent with the DSS Security Manual*

the person concerned. At this interview, the person shall be informed of the reasons for doubt, to the fullest extent possible without jeopardizing classified assets or sources of information, and shall be given an opportunity to resolve the doubt.

- 6.2.5. After such consultation and discussion, the employer, where appropriate and possible, should take steps to ensure that there is no adverse effect on the person concerned.
- 6.2.6. In cases where a clearance has been granted and reliability or loyalty of a person is subsequently placed in doubt, action shall be taken to preserve security including, if necessary, the suspension of reliability or security clearances and denial of access to classified assets by the person pending resolution of the doubt.
- 6.2.7. In the application of this section, the DSS shall ensure that the procedures which apply within the public service are followed as nearly as possible, recognizing that the employer has the sole jurisdiction and responsibility for the engagement and termination of the services of the employee and for the determination of need for access to classified assets by the employee .

### 6.3. Identification of Personnel

- 6.3.1. Non-government personnel who are employed at a non-government facility under contract with the government and who have access to classified assets should, where practicable, be in possession of an approved identification card which is issued by the contractor and which conforms to the criteria in Section 3.3. above.
- 6.3.2. The contractor, where applicable, shall implement procedures for the regular review and update of identification cards for all personnel employed who have access to classified assets. These cards will terminate when the individual's need for access to classified assets ceases.
- 6.3.3. The contractor shall ensure that inventory control and security of identification card stock are in accordance with the highest designation associated with the area in which the cards are to be used.

### 6.4. Security Education Program

- 6.4.1. A department or agency intending to enter into a contract or agreement, which involves access to classified assets, with a private sector firm shall specify in the contract or agreement that a security education program, as prescribed by the Security Branch (Supply Administration) of DSS, shall be established. This program must be similar to that described in 4.1.2.

### 6.5. Acknowledgement of Security Responsibilities

- 6.5.1. Employees, as well as other personnel under the control of, but not employed by the Contractor, who have access to classified assets, shall sign a declaration indicating their attention has been drawn, by the Security Branch (Supply Administration) of the DSS to any statutes designated by the customer department or agency as affecting the security of classified assets.
- 6.5.2. Non-government personnel shall sign the Oath of Secrecy before a Commissioner for Oaths before they are given a clearance for access to classified assets. The Security Branch (Supply Administration) of the DSS shall also ensure that they sign a declaration indicating that their attention has been drawn to the provisions of the Official Secrets Act.

.../20

007301

CONFIDENTIAL

ANNEX B

CRITERIA FOR GRANTING SECURITY CLEARANCES

A security clearance shall not be granted to the following:

- a) a person whose loyalty is in doubt because in the opinion of the deputy head the person
  - i) is or has engaged in or is planning to engage in, or
  - ii) is or has been a member of an organization or, by his or her words or actions, supports or supported an organization engaged in or planning to engage in any of the following activities:
    - 1) acts of espionage or sabotage;
    - 2) activities directed toward gathering intelligence contrary to the best interests of Canada;
    - 3) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
    - 4) activities directed toward actual or potential attack or other hostile acts against Canada;
    - 5) activities directed toward the commission of terrorist acts in or against Canada;
    - 6) activities evidencing a commitment to an ideology, a cause, a movement, or a foreign interest detrimental to or directed toward the subversion of democratic government, institutions or processes as they are understood in Canada;
    - 7) activities directed toward the creation of civil disorder in relation to any of the activities referred to in sub-paragraphs 1) to 6) above.
- b) a person whose reliability is in doubt because the person may be indiscreet, dishonest or vulnerable to blackmail or coercion, as a result of:
  - i) uncontrolled indebtedness, lifestyle, gross and continuing abuse of alcohol or drugs, continuing mental instability or criminal activity, greed or such other feature of character as might seriously affect his/her reliability;
  - ii) family or other close relationship with
    - 1) a person who is a person as described in sub-section a), or
    - 2) a person who is living in a country whose government may use such relationship for purposes prejudicial to the safety or security of Canada, unless after careful consideration of the circumstances, including the value of the person's services, the risk involved seems justified in the opinion of the deputy head, and
- c) a person whose loyalty or reliability is in doubt, because the person
  - i) is or has engaged in or is planning to engage in, or
  - ii) is or has been a member of an organization or, by his or her words or actions, supports or has supported an organization engaged in or planning to engage in

*This needs  
msj or re - w/dms*

.../

007302

CONFIDENTIAL

*open & legal?*

activities directed towards the break-up of Canada as a political entity, unless, after careful consideration of the circumstances, including the nature of the responsibilities of the position concerned, the risk involved seems justified in the opinion of the deputy head.

007303