

CSIS OPERATIONAL MANUAL

II.3 SECURITY SCREENING

A. SUBJECT

- A. 1. This chapter deals with security screening procedures.

B. REFERENCES

- B. 1. Public Service Employment Act Regulations
- B. 2. Access To Information/Privacy Act
- B. 3. Immigration Act (1976) and Regulations
- B. 4. Immigration Manual
- B. 5. Financial Administration Act
- B. 6. Canadian Human Rights Act
- B. 7. Criminal Records Act
- B. 8. Cabinet Directive 35
- B. 9. Security Panel (SP)243
- B. 10. Cabinet Directive 28-81RD(c)
- B. 11. Canadian Security and Intelligence Service Act
- B. 12. Citizenship Act

C. POLICY

- C. 1. The Solicitor General shall be kept informed of all cases which may come to public notice or may be subject to discussion at the ministerial level.
- C. 2. All personal information to be disclosed outside the Service shall be provided in writing and shall require the approval of the Director General, Security Screening, before release.

CSIS - SCRS
Records Dossiers

APR 23 2004

Revisé
Reviewed

A0145227_1-000246

C. POLICY (cont'd)

- C. 2. a. The approval of the appropriate Deputy Director is required when an operational branch objects to disclosure.
- C. 3. The screening process shall not be used as a lever for source development or as a pretext to further any other operational interests.
- C. 4. If requested by a federal government institution, a security clearance investigation shall be conducted promptly on all applicants for, and employees of the public service who are required to have access to assets classified in the national interest.
- C. 4. a. Information obtained from the investigation shall be used to assess the person's loyalty and reliability as it relates thereto.
- C. 5. Federal government security clearance procedures on behalf of any individual, company, police force, provincial or municipal government department or agency shall only be conducted through and upon request of a federal institution.
- C. 5. a. Where doubt exists as to the level or the propriety of a request for a security clearance, the originator shall be challenged to justify the inquiry under C.D. 35., see also Appendixes II-3-1 and II-3-2.

C. POLICY (cont'd)

- C. 6. Sources who admit homosexual activity shall not be reported on or made subject of a file on the basis of that admission alone.
- C. 7. Information that a person does or may advocate separatism shall not be sought but shall be reported if it is made available.
- C. 8. Results of an investigation shall be provided in a factual report which includes:
 - C. 8. a. a clear statement whether the candidate should or should not be allowed access to classified material, and
 - C. 8. b. an evaluation of the sources used regarding the reliability of the information they have supplied.

D. GENERAL

- D. 1. The suitability of a person for access to classified assets is not only determined by his/her loyalty, but also by his/her reliability as it relates thereto.
- D. 2. When conducting field investigations, investigators should conduct the most thorough investigation possible into the character, lifestyle, loyalty and background of a candidate so that the department concerned may have a factual basis on which to determine his/her suitability for employment to handle classified assets.

E. STANDARDS OF SECURITY CLEARANCE

E. 1. GENERAL

E. 1. a. Personal information necessary for security screening inquiries is usually provided by the department concerned on a Personal History Form (PHF) and is collected under authority of Section 26 of the Public Service Employment Act Regulations.

E. 2. Security clearance investigations may be conducted and information disclosed to government institutions in response to requests for clearances in the following categories:

E. 2. a. Cursory - involves a check of subversive indices on the basis of the information supplied.

E. 2. b. Confidential - requires:

1. a check of fingerprint and subversive indices,
2. foreign agency indices if applicable, or
3. a field investigation, including a check of credit bureau records, if there is sufficient cause or where requested by a DSO.

E. 2. c. Secret - same as E.2.b.

E. 2. d. Security Panel SP (243) (Applies to Canadian Corps of Commissionnaires employed in the National Capital Region) - requires:

1. a check of fingerprint and subversive indices,
2. a check of credit bureau records,

**E. STANDARDS OF SECURITY CLEARANCE
(cont'd)**

- E. 2. d. 3. a field investigation covering the immediately preceding three years, excluding Department of National Defence and Canadian Corps of Commissionnaires employment, and
4. a check of foreign agency indices if applicable.

E. 2. e. Top Secret - requires:

1. a check of fingerprint and subversive indices,
2. a check of credit bureau records,
3. a check of foreign agency indices if applicable, including field inquiries, and
4. a field investigation covering the immediately preceding ten year period or to the candidate's 18th birthday.

NOTE: For RCMP, CSIS and DND employees or applicants, the investigation is to be to the candidate's 16th birthday.

E. 2. f. Special Activity (SA) - requires:

1. a check of fingerprint and subversive indices,
2. a check of local law enforcement agency records in locations where the candidate has resided for substantial periods of time if no legislative prohibition exists.

**E. STANDARDS OF SECURITY CLEARANCE
(cont'd)**

- E. 2. f. 3. a check of credit bureau records,
4. a check of foreign agency indices if applicable, including field inquiries, and
5. a field investigation covering the immediately preceding 20 year period or to the candidate's 18th birthday.

NOTE: For RCMP, CSIS and DND employees or applicants, the investigation is to be to the candidate's 16th birthday.

- E. 3. The decision as to which category of clearance applies rests with the requesting government institution and is based upon the nature of the position the candidate is being considered for and the classification of the assets to which he/she is expected to have access.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS

F. 1. Policy

- F. 1. a. Personal information shall only be collected or disclosed to a government institution when it relates to the suitability of:
1. an individual for access to assets classified in the national interest, or
2. a person to hold a high public office as provided for in F.7.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 1. b. Disclosure of information obtained through a security clearance inquiry shall be to the Departmental Security Officer (DSO) or to the deputy head of the institution when the DSO is the subject of the inquiry or where the case is particularly sensitive.

EXCEPTION: As provided for in F.7.b.6.2. regarding cursory records checks on certain government officials.

- F. 1. c. For the purposes of security screening, a subversive indices check does not include:

1. [REDACTED] category files, or

2. [REDACTED]

- F. 1. d. In situations where there is reason to believe that information of value may exist on other than [REDACTED] files, all available records will be checked, see also F.7.

F. 2. General

- F. 2. a. The Service is, upon request, responsible for providing a security assessment of the loyalty to Canada and reliability as it relates to:

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 2. a. 1. candidates for or incumbents of positions in federal government institutions who are intended or expected eventually to have access to assets classified in the national interest,
2. persons charged with the security of facilities where classified assets are retained,
3. employees of provincial or municipal governments with access to classified federal government assets,
4. persons in the private sector involved in or engaged upon the production or study of classified defense equipment,
5. persons who are not intended to have access to classified assets but who, due to their work environment, may have unintended access or where unintended access is a reasonable possibility,
6. prospective ministers, senators and parliamentary secretaries,
7. order-in-council appointees of the federal government,
8. minister's exempt staff, and
9. employees of companies involved in contracts of a classified nature with the Service.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 3. Security Screening

- F. 3. a. Follow the procedures in Appendix II-3-3.

F. 4. Criminal Records

F. 4. a. Policy

1. A criminal record which has been subject of a pardon shall only be disclosed with the consent of the Solicitor General.
2. A criminal record shall only be reported as fact to a DSO when it has been confirmed by a comparison of fingerprints.

F. 4. b. General

1. A check of criminal records is normally performed when the DSO submits a request directly to RCMP "I" Directorate.

F. 4. c. Security Screening - Screening Unit

1. When a criminal record is discovered on a candidate of a screening inquiry:
 1. Obtain all relevant information from RCMP "I" Directorate.
 2. Determine from the responsible DSO if the candidate is employed in a position falling within the categories listed in F.2.a.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 4. c. 1. 3. Advise the DSO to update the candidate's security record by forwarding fingerprints to RCMP "I" Directorate, Identification Services, Civil Section, if it is confirmed that the candidate has access to classified material except for F.2.a.7., F.2.a.8. and F.2.a.9.
4. For cases falling within F.2.a.7., F.2.a.8. and F.2.a.9., bring all details to the attention of the Director and follow the procedures in F.7.
5. Determine whether the criminal record has been subject of a pardon.
6. Together with the Security Screening [REDACTED] Unit assess the relevance of the record, including the circumstances of the intended employment, when:
- the criminal record has been pardoned,
 - an absolute discharge has been registered,
 - a criminal investigation did not lead to charges being laid, or
 - a warrant for the candidate's arrest is outstanding.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 4. c. 2. When a criminal record has been pardoned but it is judged directly relevant to security:

1. Seek a Ministerial Waiver through RCMP "I" Directorate as provided for in Section 6(2) of the Criminal Records Act,
 2. Withhold your report to the DSO pending a decision whether or not the record may be disclosed, and
 3. Notify the DSO that a reply will be delayed.
3. When a pardoned criminal record is judged not relevant to the candidate's security status or when no Ministerial Waiver is obtained:
1. return the record to RCMP "I" Directorate without retaining any copy or record thereof, and
 2. process the report to the DSO in the normal manner.

NOTE: When it is necessary to maintain a record of a pardoned criminal offence, request Records Management to seal the record on the candidate's file and mark it to be opened only by the Deputy Director General, Records Management.

4. When a criminal record that has been reported to a government institution by Headquarters Security Screening or its predecessor, "A" Operations, is subsequently pardoned, follow the instructions in SSOM IV.4.K.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 4. c. 5. When a warrant is outstanding on a person holding or requiring a security clearance, contact the agency holding the warrant through the appropriate regional office on an urgent basis to determine:
1. if the candidate is identical to the person named in the warrant,
 2. the circumstances of the offence for which the warrant was issued, and
 3. what action has been taken or is intended to be taken to execute the warrant.
6. Forward all pertinent information concerning the outstanding warrant to the Headquarters Security Screening [REDACTED] Unit for the notification of the DSO.
7. When no fingerprints have been submitted to RCMP "I" Directorate and the warrant is returnable, notify the Director of Criminal Investigations (DCI) in writing.

F. 5. Foreign Agency Checks

F. 5. a. Policy

1. Only information necessary to permit a proper inquiry shall be disclosed to an approved foreign agency when requesting checks be conducted.

F. 5. b. General

1. Foreign agency inquiries are performed on the basis of reciprocal agreements and are carried out to the extent permitted by local legislation and availability as set out in the Immigration World Index - Part I.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 5. b. 2. Foreign agency checks are normally conducted:

1. in those countries where reciprocal agreements exist or facilities are otherwise available,
2. on the subject of inquiry and those persons known to have a close and continuing relationship with him/her, e.g. a spouse.
3. on persons who have resided outside Canada in excess of one year in a capacity other than as an employee of the federal or a provincial government.
4. to resolve doubt or clarify traces, and
5. as otherwise specifically requested by the DSO.

F. 5. c. Headquarters Security Screening

1. In the case of the USA, Great Britain and Bermuda, submit requests for checks directly to the agency concerned.
 1. In all other cases, submit requests to the SLO at the designated post.
2. Notify the DSO of the time required before a reply from a foreign agency can be expected.
3. Provide to the foreign agency concerned only as much personal information about the candidate as is necessary to permit proper inquiries.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 5. c. 4. Provide the DSO with revised time estimates when foreign agency checks exceed the original time estimate.

F. 6. Credit Bureau Inquiries

F. 6. a. Policy

1. All searches of credit bureau records on behalf of government institutions shall be conducted in writing by Headquarters Security Screening.
2. All user fee charges shall be verified monthly against a log of security screening cases maintained for that purpose.
3. Information obtained from credit bureau records shall only be disclosed for purposes of employment or as otherwise provided for in Sec. 8(2) of the Privacy Act where no specific legislative prohibition exists.

F. 6. b. General

1. In accordance with CD 35, the Service is responsible for conducting a check of credit bureau records for all requests for top secret security clearance or as otherwise deemed necessary to ensure that the subject of inquiry is a person in whom the federal government can place full trust and confidence.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 6. c. Investigator

1. If you believe that information relevant to your security clearance investigation is available at a local credit bureau office and that inquiries have not been initiated, request the necessary checks be conducted by Headquarters Security Screening.

F. 6. d. Head Regional Office Records Management

1. Upon receipt of all credit bureau information, seal it to be opened only by the supervisor of security screening investigations and place it on the appropriate file.

F. 6. e. Headquarters Screening Analyst

1. Conduct a check of credit bureau records at the location of the most recent address shown on the candidate's Personal History Form (PHF) or as otherwise deemed advisable.
2. Complete, sign and forward a Service Request Coupon to the Security Screening, Administration Clerk.
3. On receipt of the credit bureau report, submit it to the Security Screening, Admin. Clerk for logging and forward significant details of the report to the regional office involved in the investigation.

F. 6. f. Headquarters [REDACTED] Analyst

1. When the investigation is complete and a security clearance assessment has been forwarded to the DSO:

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 6. f. 1. 1. Destroy all credit bureau reports which do not contain reportable information.

2. Seal all reported credit bureau information and the file copy of the security clearance assessment and place it on the appropriate file, to be opened only by supervisors of the Headquarters Screening or [REDACTED] Units.

F. 6. g. Security Screening Administration Clerk

1. Log all credit bureau requests and forward them by mail to the appropriate credit bureau.

2. Upon receipt of the credit bureau report, log it then forward it to the screening analyst.

3. Verify each credit bureau report invoice with the log at the end of each month and bring any irregularities to the attention of your supervisor.

4. When the credit bureau invoice is considered accurate, have it certified by your supervisor and forward it to Headquarters Financial Services.

F. 6. h. Headquarters Financial Services

1. If the credit bureau invoice is accurate and properly certified, remit payment.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 7. Cursory Records Checks

F. 7. a. Policy

1. The Screening Unit shall be responsible for conducting a cursory check of:

1. subversive and criminal (CPIC) indices upon an oral or written request from a DSO in respect to a person identified as a nominee for a ministerial exempt staff position, and

2. subversive indices upon the written request from the Commissioner of the RCMP or his designate, in respect to:

- prospective ministers
- parliamentary secretaries
- senators, and
- nominees for Order-In-Council appointments outside of Parliament.

NOTE: the written request may be preceded by a telephone call if the circumstances warrant it.

2. All requests for cursory checks shall be processed urgently on a strict need-to-know basis.

3. Investigative action concerning nominees for Order-In-Council appointments shall not be initiated on the basis of a cursory record check unless expressly authorized by the Director.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 7. b. Screening Unit

1. When no reportable traces are discovered for ministerial exempt staff nominees:

1. Notify the DSO by telephone.
2. Prepare a written confirmation for the signature of the Director General, Security Screening.

2. When no reportable traces are discovered for prospective ministers, parliamentary secretaries, senators and nominees for Order-In-Council appointments:

1. Prepare a written reply to the Commissioner of the RCMP.
2. Provide telephone notification in advance of the written response only when circumstances dictate.

3. Where reportable subversive traces are discovered for ministerial exempt staff nominees:

1. Ensure a check [REDACTED] indices is made.
2. Notify the DSO a response will be delayed and request a PHF, appropriately certified as to requirement and level of access to classified assets, be forwarded to the Service.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 7. b. 4. Upon receipt of the appropriate documents, open a security screening [REDACTED] file if one does not already exist and proceed as set out in F.8.

5. When criminal traces are found and are believed to be identical to the subject of enquiry, prepare a reply to the DSO:

1. setting out the details of the traces;
2. qualifying the identification factors, and
3. pointing out that positive identification of the trace to the subject can only be confirmed through a comparison of fingerprints.

6. Where reportable subversive traces are discovered in respect to prospective ministers, parliamentary secretaries, senators and nominees for Order-In-Council appointments:

1. Ensure a check [REDACTED] indices is made.
2. Prepare a reply to the Commissioner of the RCMP notifying that the matter will be addressed by the Director with the applicable DSO or Clerk of the Privy Council as required.
3. Have a security screening file opened if one has not already been opened.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 7. b. 6. 4. Forward the traces to the Security Screening [REDACTED] Unit for an urgent security assessment.

F. 7. c. [REDACTED] Unit

1. Access all relevant security traces.
2. Prepare a detailed security assessment, qualifying the information when:
 1. time does not permit full checks, or
 2. the lack of biographical data does not permit positive identification.
3. Determine access restrictions in accordance with IV.4.J.

F. 7. d. Records Management

1. Upon request from the DG, Security Screening, conduct a subversive indices check.
2. Upon request from the DG, Security Screening, open a security screening file, notwithstanding the existence of another [REDACTED] file.
3. Ensure future access to the subject's file is restricted as indicated by the DG, Security Screening.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. Field Investigations

F. 8. a. Policy

1. In all cases where investigative action is required, the individual shall be made subject of a [REDACTED] file.
1. No information unrelated to the security screening is to be carried on the candidate's file.
2. When the subject of inquiry has not resided in Canada long enough to permit reliable inquiries, he/she and any references given shall be interviewed to determine whether their first loyalty is to Canada.
3. Only experienced, mature investigators shall be employed on security screening duties.
4. Local RCMP detachments shall conduct security screening investigations in locations where, in the judgement of the Director General Regional Office, it is impractical for Service units to do so.
5. Every effort shall be taken during the course of security screening inquiries to ensure that the individual described by sources is identical to the subject of the PHF.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. a. 6. Information relating to a candidate's character or life style shall not be collected or carried on the candidate's file unless it relates directly to:

1. the security screening pursuant to CD 35.
7. Information that a candidate does or may advocate separatism shall not be sought or expanded upon intentionally during a security clearance investigation but shall be reported if it is made available.
8. Where subversive traces have been developed, the candidate of the inquiry shall be interviewed wherever possible keeping in mind the sensitivity of sources involved and other operational considerations.

F. 8. b. General

1. Indications of fundamental disloyalty to Canada e.g., involvement in espionage, terrorism, subversive organizations, will, in most cases, be surfaced through a search of subversive indices rather than through a screening investigation. The primary value of the field investigation is in determining whether a person's character or life style could lead the candidate into indiscretion, dishonesty, or render him/her vulnerable to compromise or blackmail.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. b. 2. A thorough field investigation must be conducted and a detailed report submitted to:

1. provide the department or agency concerned with sufficient background information on the candidate so a conscious judgement can be made regarding his/her trustworthiness,

NOTE: A summary or statement that nothing adverse has emerged from the enquiries does not provide the depth of information required to allow the departmental official, in arriving at a decision, to compare favourable against unfavourable information.

2. ensure screening inquiries being updated allow for a current assessment of the candidate and that previous enquiries conform to present standards, and
3. detect discrepancies between the views expressed by sources and statements made by the candidate.

NOTE: Discrepancies may indicate untruthfulness resulting in further inquiries being necessary.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. b. 3. While the Department of National Defence (DND) and the RCMP normally conduct their own field investigations, any designated federal government institution may request a field investigation:

1. on persons being cleared for access to top secret,
 2. on persons being cleared for access to Cabinet documents;
 3. for members of the Canadian Corps of Commissionnaires employed in the National Capital Region,
 4. on persons who are employed in areas vital to national security where unintended access is a reasonable possibility,
 5. to resolve doubt in accordance with paragraphs 15 and 25(ii)(b) of CD 35,
 6. to clarify traces, or
 7. as otherwise considered necessary by the DSO.
4. Except for RCMP and DND employees where enquiries extend to a person's 16th birthday, field investigations do not normally go beyond the candidate's 18th birthday, but otherwise, are expected to cover:
1. a period of ten years,
 2. a period of 20 years for persons intended to have SA clearance,
 3. a period of 3 years for members of the Canadian Corps of Commissionnaires employed in the National Capital Region, and

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 8. b. 4. 4. a period of ten years for members of the Canadian Corps of Commissionaires being cleared to top secret when requested by the employing institution.

F. 8. c. Headquarters Security Screening

1. Conduct credit bureau checks and initiate or request CPIC checks.
2. Specify to the regional office the type of investigation e.g., clearance to SA standards, and provide:
 1. a PHF for the candidate together with any consent form attached thereto,
 2. any trace information,
 3. the results of credit bureau checks as soon as they are known,
 4. any criminal record traces as soon as they are known,
 5. any specific investigational instructions,
 6. the name, if any, of other regional offices involved in the investigation, and
 7. a diary date.
3. Use the appropriate operational file to correspond when the investigation is to clarify subversive traces or to determine influence factors.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 8. c. 4. Correspond on the candidate's [REDACTED] file when the investigation is to clarify reliability as it relates to loyalty.
5. If a DSO requests a field investigation to clarify allegations or suspicions of involvement in separatist activity, inform him that such investigations are not mandated for and take no further action.
 6. When the subject of the investigation falls within the provisions of F.8.a.2., instruct the regional office to proceed accordingly.
 7. When the subject of the investigation is an employee of, or candidate for the Service, request the regional office to be alert to employment suitability factors and interview all references listed.
 8. When the diary date has not been complied with, request an immediate report from the regional office.
 9. When a report is received from the regional office, review it for thoroughness, objectivity and relevance and ensure every reasonable effort has been made:
 1. to corroborate adverse information,
 2. to ensure identification,
 3. to resolve any doubt,
 4. to clarify subversive traces, and
 5. to properly assess the information provided by all sources.
 10. If a report is considered inadequate, provide appropriate direction to the regional office.

A0145227_26-000271

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. d. Director General Regional Office

1. Allow only security screening investigations requested by Headquarters Security Screening to be conducted.
2. When it is impractical for Service personnel to conduct an investigation, have all pertinent information forwarded to the appropriate RCMP detachment and assign a suitable diary date.
3. To the fullest extent possible have only mature, experienced investigators assigned to security screening inquiries.
4. Have all inquiries necessary to clarify or amplify subversive traces conducted by an investigator with the appropriate expertise.
5. Ensure a consistently high quality investigation is conducted by your personnel and that diary dates are respected.
6. Ensure a statistical record of security screening investigations conducted is maintained.
7. As you deem necessary, establish and maintain a liaison program with:
 1. regional security officers,
 2. security officers in private industry, and
 3. local law enforcement agencies.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. e. Investigator

1. Not every element will be present or the same in every case, therefore common sense is still the best guide to uncovering relevant information during a field investigation.
2. Carefully review the candidate's PHF as well as any related documentation and establish a plan of action.
3. When practical, consult telephone or city directories or similar publications to verify addresses and establish possible sources of information.
4. When possible, conduct checks of intended sources through CSIS indices.
5. While there is no requirement to check RCMP Division CIB records on persons other than the candidate, you may do so for close relatives, associates and sources where you feel it may contribute to an understanding of the subject or help in the assessing of information.
6. Conduct a check of local police records when:
 1. the candidate may have been convicted of a criminal offence,
 2. a warrant is outstanding,
 3. the candidate may have criminal associates,
 4. it is necessary to clarify information or assess sources,

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 8. e. 6. 5. when specifically directed to do so, or

6. when you feel it practical and worthwhile to do so.

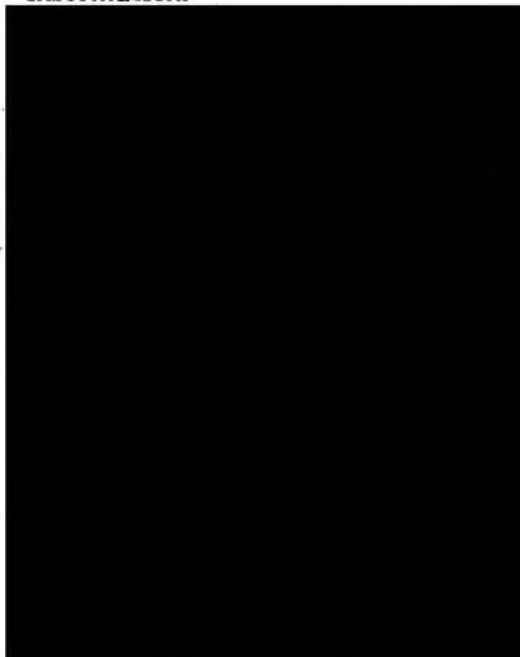
7. If you wish to conduct credit bureau checks, follow the procedures in F.6.c.

F. 9. Inquiries and Interviews

F. 9. a. Investigator

1. When it is necessary to take a PHF on an investigation, take appropriate security precautions to prevent accidental disclosure of the contents and do not show it to sources.

2. When making inquiries, consider the following sources of information:



F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 9. a. 3. To the fullest extent possible, interview only respected, responsible members of the community who have personal knowledge of the subject of inquiry.

4. Make every effort by telephone to arrange appointments for interviews with sources and:

1. Fully explain the reason for the inquiry and the importance to the security of Canada of obtaining an informed, unbiased, truthful appreciation of whether the candidate is a person in whom the government may place full trust and confidence.

2. Establish whether the source knows the candidate well enough to assist the investigation.

3. If the source agrees, arrange a convenient time to meet.

NOTE: Avoid conducting any part of the interview by telephone unless the source insists, then include the circumstances in your report.

5. If a source is hesitant about providing information, fully explain the protection provided for sources as found in sections 22 and 23 of the Privacy Act.

6. Attempt to put the person being interviewed at ease and keep questions brief, uncomplicated and unthreatening.

7. During an interview, take precautions to ensure all sources, methods of operations and targets are protected to the fullest extent possible.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 9. a. 8. While circumstances will dictate the approach to be taken during an investigation, ensure that all inquiries and interviews relating to traits of character, lifestyle or personal circumstances, e.g. homosexuality, venality, alcoholism, debt, or gambling, are conducted with sensitivity, tact, discretion, maturity of judgement and absence of bias.

1. Ask source for specific examples of why the candidate is considered to be dishonest, indiscreet, etc., so a full appreciation of the context in which the opinions are offered can be assessed.

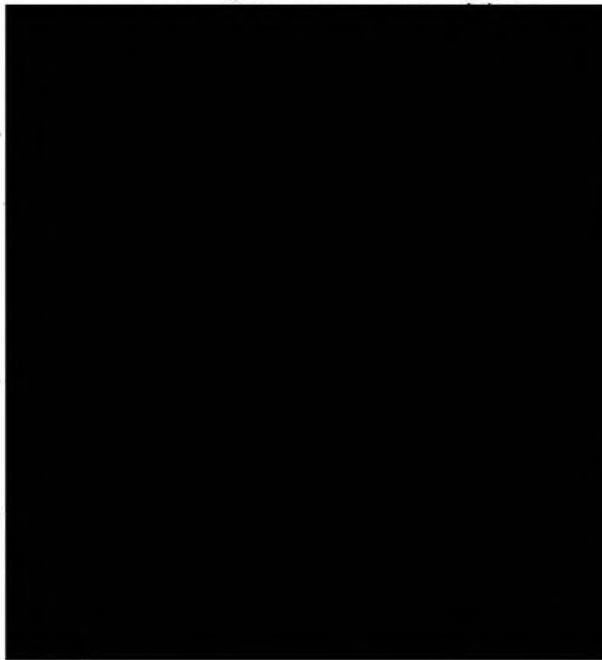
NOTE: It will often be difficult for sources to provide evidence of a person's honesty, discretion, loyalty, etc., therefore they should be asked to describe any incidents of dishonesty, indiscretion or doubtful loyalty of which they have knowledge.

9. Where a source is in a position to appreciate the importance of access to classified information, seek the source's opinion, based on the reasons he/she has given, whether the candidate should be granted a security clearance.

10. When adverse information surfaces during an inquiry, attempt, to the fullest extent possible, to corroborate it.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 9. a. 11. Explore fully how the candidate copes with an alternate lifestyle, e.g. homosexuality, emphasizing whether he or she is embarrassed or secretive about it and if vulnerable to compromise, blackmail or indiscretion.
12. Do not attempt to obtain access to health, income tax, financial records, or any other records where access may be prohibited by law or a professional code of ethics unless you have obtained the specific consent form from the individual to whom the record refers.
13. When making inquiries or conducting an interview, explore:

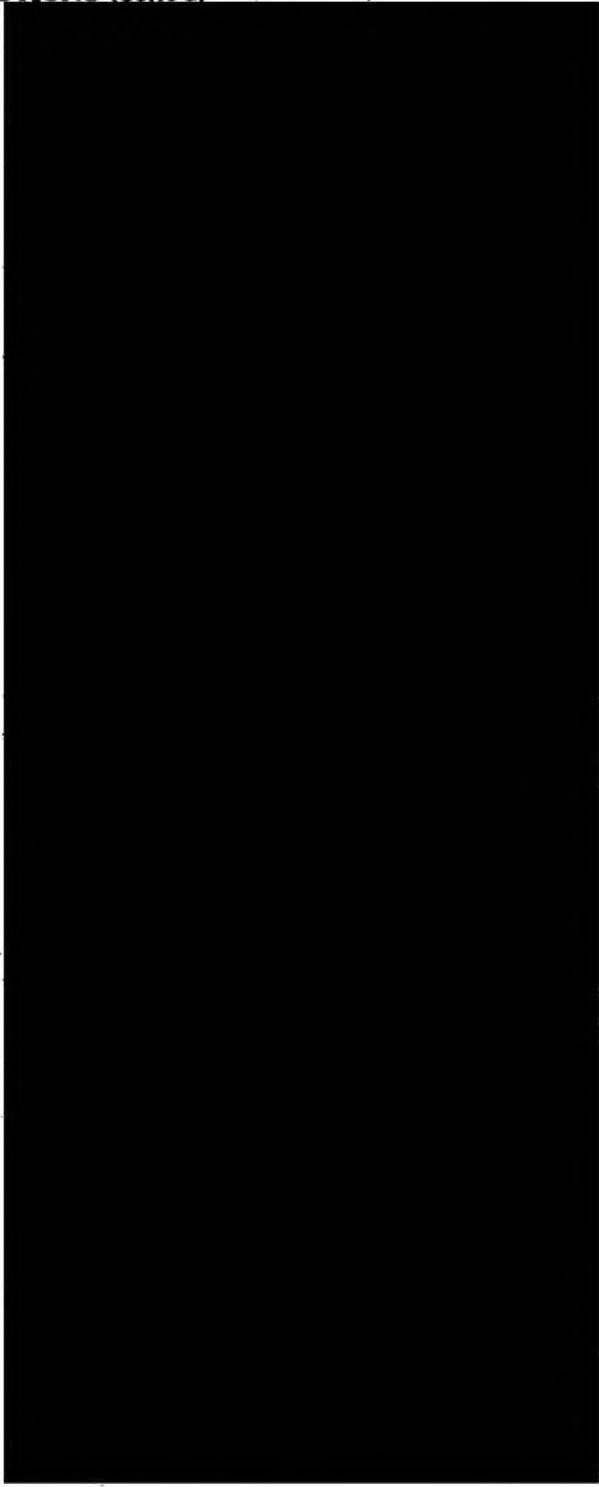


s.15(1)

s.16(1)

● **F. GOVERNMENT SCREENING - FEDERAL
INSTITUTIONS (cont'd)**

F. 9. a.



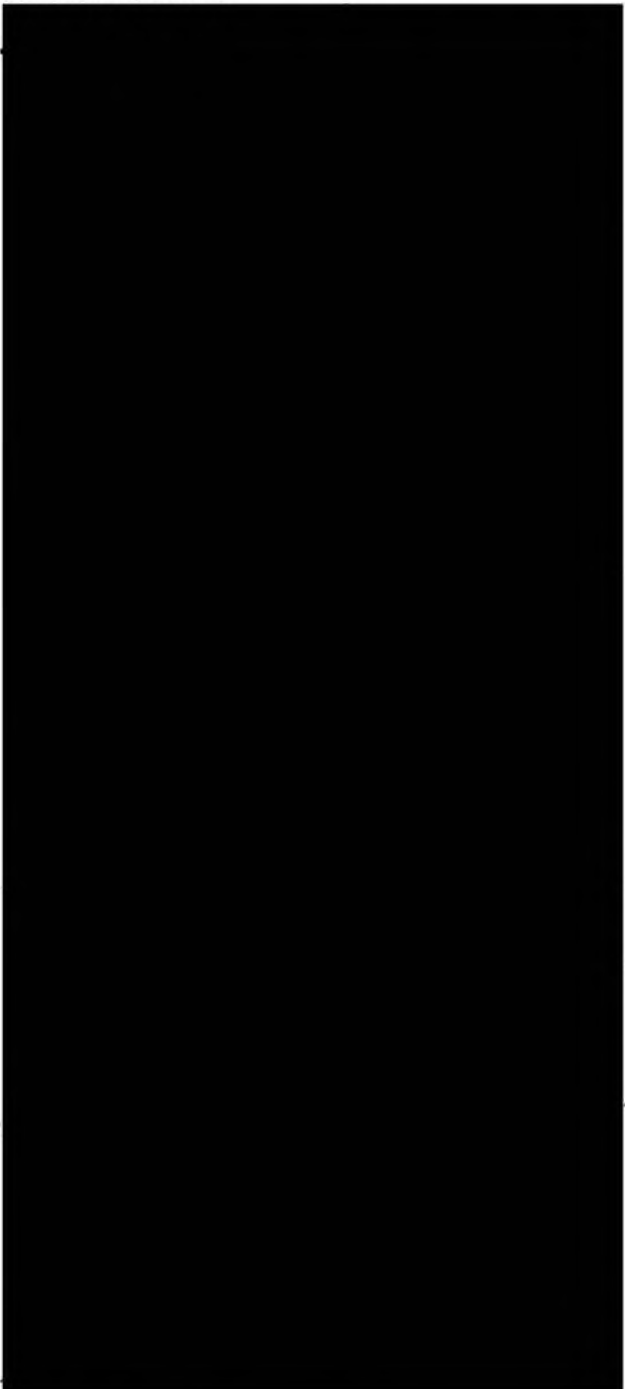
A0145227_33-000278

s.15(1)

s.16(1)

**F. GOVERNMENT SCREENING - FEDERAL
INSTITUTIONS (cont'd)**

F. 9. a.



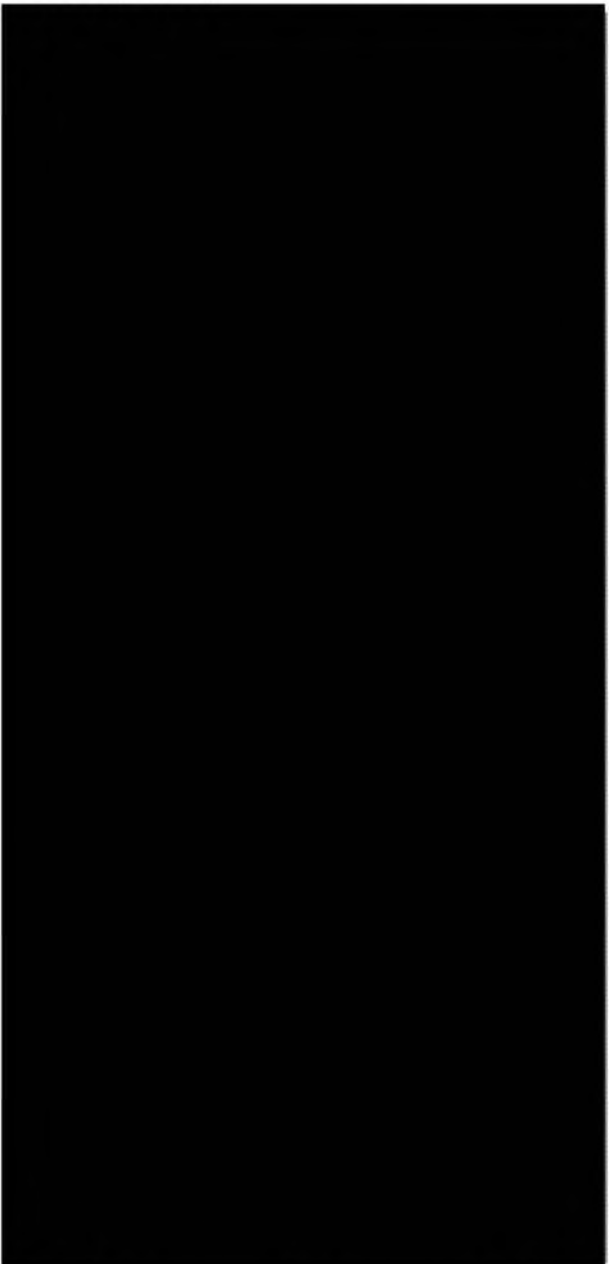
A0145227_34-000279

s.15(1)

s.16(1)

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 9. a.



33. When adverse security information surfaces, request approval from Headquarters Security Screening to interview the candidate to:

1. provide the person an opportunity to explain his/her actions or refute any allegations, and

A0145227_35-000280

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 9. a. 33. 2. provide the investigator with an opportunity to

[REDACTED] come to his/her own opinion whether the candidate should be given a security clearance.

- F. 9. a. 34. In cases where consideration is being given to downgrading or removing a candidate's security clearance (FOR CAUSE), ensure adequate protection, pursuant to Section 22(1)(b) of the Privacy Act, is afforded sources used in the investigation by establishing at the outset of an inquiry or interview whether the information being provided is in confidence and indicate this in your report.

35. If, in the course of your inquiries, you believe that a complaint may be lodged against you or that criticism concerning the investigation will be forthcoming, immediately provide Headquarters Security Screening with a report outlining all the circumstances.

F. 10. Reporting

F. 10. a. Investigator

1. Report all information developed which is relevant to determining whether a candidate should be given a security clearance. See also Appendix II-3-4 for format.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 10. a. 1. 1. When the investigation is for an employee of the Service, submit a separate report to the Director General Personnel Services containing any positive or negative information which would assist in determining the candidate's suitability for employment.
2. When certain circumstances about a candidate are believed to exist and you are satisfied the information is true although not corroborated, clearly indicate this in your report.
3. When you do not know whether or not to believe the comments of a source, indicate in your report that the information is unverified and is being reported without any assessment as to its reliability.
4. Avoid any subjective comments regarding whether the candidate should be afforded access to classified material.
1. Provide comments where you have been able to form a valid opinion during the investigation concerning whether the candidate's character, beliefs, or lifestyle could have a bearing on his or her loyalty.
5. Provide a full assessment of all sources used in the investigation and include:
1. their relationship to the candidate, i.e. social, coworker, recreational or casual,

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 10. a. 5. 2. the apparent knowledge of the candidate over what period of time,
3. any indication of dishonesty or bias in reporting for or against the candidate,
4. the basis for any belief or opinion expressed, and
5. the expectation of confidentiality as provided for in F.9.a.34.

F. 10. b. Regional/District Office Records Management

1. Place the regional/district office copy of an investigator's report and all related documentation on file.
 1. BF the file to ensure the return of the detachment report.
2. Retain the security investigation correspondence in accordance with the appropriate disposition schedule.

F. 10. c. Regional Director General/District Chiefs/Heads

1. Ensure secure communications facilities are used to transmit security screening reports to Headquarters.
 1. If you do not have access to secure facilities, use appropriate CSIS stationary.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 11. Preparation of Intelligence Assessment

F. 11. a. General

1. A subject of security screening procedures may make application under the Privacy Act to see the intelligence assessment, together with any related report or document, provided to the government institution. This should not cause concern about incurring civil liability so long as all members involved have conducted themselves properly and without malice within the performance of their public duty. Reporting something as true when one knows it to be untrue could constitute malice. A member engaged in security screening duties will not incur liability for slander or libel if:

1. he reports only to those persons to whom he has a duty to report, and
2. he confines his comments to accurate statements concerning what he has been told, and any verification or lack of it.

F. 11. b. Headquarters [REDACTED] Unit

1. Prepare an intelligence assessment for the DSO including only those allegations or facts which are reported and where identification is based on information, the reliability of which has been properly assessed.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 11. b. 1. 1. Include as an attachment any relevant open information which can be safely disclosed, e.g. newspaper clippings.
2. Describe in the intelligence assessment the activities of the candidate in relation to his/her loyalty pursuant to paragraphs 3 and 4 of CD 35.
1. Report, as much as is possible, only activities that have been corroborated by independent sources.
3. Where the candidate has at one time been a member or supporter of an organization described in paragraph 3 of CD 35, describe to the fullest extent known, his or her reasons for discontinuing the membership or support.
1. When including information that a candidate may support separatism, ensure that the information is fully qualified in terms of its reliability and the time span involved.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 11. b. 4. Where the candidate has a close continuing relationship with a family member or other associate and that individual falls within the provisions of paragraphs 3 and 4 of CD 35, describe to the fullest extent possible, the degree of and circumstances surrounding the relationship, particularly the degree of influence that might be exerted on the candidate to act in a manner prejudicial to the security of Canada.
1. Except where there are reasonable grounds to believe the candidate of inquiry is under the undue influence of a close relative or associate, information relating to the reliability of the relative or associate, i.e. greed, debt, homosexuality, criminal record, or evidence of support for separatism which does not have a bearing on the security status of the candidate should not be reported or otherwise commented upon in the intelligence assessment.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

- F. 11. b. 5. Where the subject of inquiry is bound by close ties of blood or affection to residents of foreign nations, describe, to the fullest extent known, the degree of influence that might be exerted on the candidate to act in a manner prejudicial to the security of Canada.
6. When preparing the intelligence assessment, avoid, as much as possible, reliance upon information from technical or other sensitive sources.
 7. In all cases where the information reported is uncorroborated or otherwise uncertain, clearly note this in the intelligence assessment.
 8. When preparing the intelligence assessment, ensure all sources, methods of operation and targets of the Service are protected to the fullest extent possible.
 9. Provide in the intelligence assessment a full evaluation of the risk to security posed by the candidate in relation to the provisions of paragraphs 3, 4, 6(a) and 6(c) of CD 35.
 10. Include details of the interview of the candidate and a recommendation as to whether or not a security clearance should be granted.
 11. When applicable, attach to the intelligence assessment an approved profile of any organization to which the subject of inquiry or his/her close relatives or associates have belonged if the organization:

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 11. b. 11. 1. has been assigned a level of investigation by the Operational Priorities Review Committee (OPRC), or

2. is now defunct or altered in character but was, at the time of the candidate's contact or involvement, an organization which had or would have had OPRC approval.

12. Nothing in F.11.b.11. precludes including comments on the candidate's involvement in other legitimate organizations in the body of the intelligence assessment providing the involvement is relevant to the candidate's security status and it is made clear that the organization itself is not considered to be subversive in character.

13. When adverse information on a person holding a security clearance is surfaced from a sensitive source or in a current operational context:

1. Consult with the appropriate operational branch to determine the appropriate level at which the information can be disseminated.

2. Forward to the federal institution concerned any information which can be released in accordance with C.2.a. and attach form SSF 213 to the inside front cover of the appropriate operational file.

F. GOVERNMENT SCREENING - FEDERAL INSTITUTIONS (cont'd)

F. 11. c. Director General Headquarters Branch

1. Upon request, provide assessments and advice to Security Screening for cases involving your operational responsibilities.
2. Ensure operational profiles are updated and provide them to Security Screening upon request.

G. IMMIGRATION SCREENING

G. 1. Policy

G. 1. a. The Director Criminal Investigations (DCI) and the Canada Employment and Immigration Commission (CEIC) shall be notified through the Director General Security Screening of all cases where there is any indication of possible involvement in war crimes.

G. 1. b. The prior approval of the Director General Security Screening shall be obtained before any disclosure of personal information is made.

1. The Director's approval is required before disclosing information to an agency of a country which violates human rights.

1. If doubt exist whether the country violates human rights, consult with the Director General, Foreign Liaison.

G. 1. c. Only personal information directly related to the following shall be collected or disclosed to the CEIC:

1. the immigration screening process,

G. 1. c. 2. the exercise of Ministerial or Visa Officer (VO) discretion, or

3. the [REDACTED]
[REDACTED] decision.

G. 1. d. Information obtained during the screening process shall not be disclosed to a foreign agency unless:

1. it directly relates to reciprocal responsibilities; and
2. it is authorized by the appropriate operational branch and when required referred to the Director General Foreign Liaison.

G. 1. e. Records Management shall [REDACTED]
[REDACTED] when Security Screening has determined:

1. [REDACTED]
2. [REDACTED]
3. that personal information received during the screening process has been used for an administrative purpose or is intended to be retrieved in a systematic way, or
4. that outside Canada enquiries are indicated on immigration applications without prior reference to the Director General Security Screening.

G. 2. Immigrant Screening Procedures

G. 2. a. General

1. The Service is responsible for providing advice to the CEIC in accordance with the provisions of Section 19(1)(e)(f) and (g) of the Immigration Act. This applies to all persons seeking landed status in Canada between the ages of:

- G. 2. a. 1. 1. [REDACTED] in the case of family class or assisted relatives, and
2. [REDACTED] for all other classes.

2. The decision to grant or refuse landed status in Canada rests with the CEIC.

G. 2. b. Security Liaison Officer (SLO)

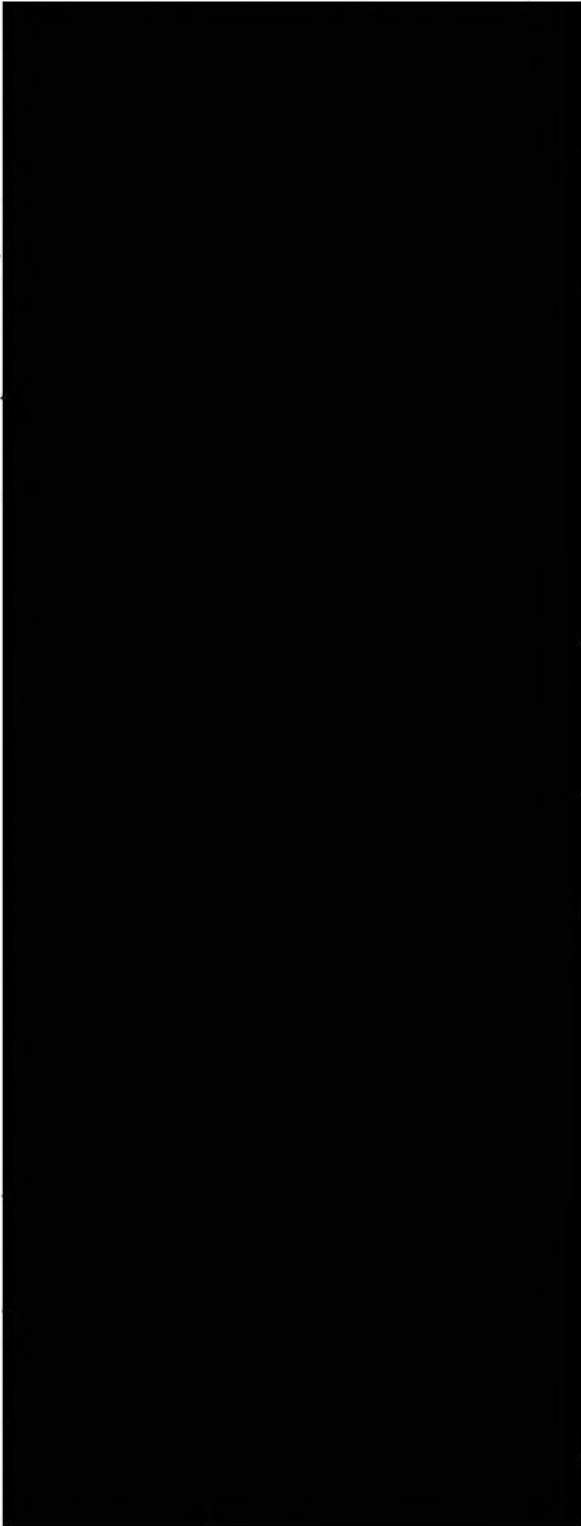
1. To allow for proper security inquiries, ensure that sufficient information is included on the "Application for Permanent Residence" form Imm. 8. Refer to the Immigration World Index - Part I.
2. Unless extenuating circumstances exist, make every effort to ensure Immigration is notified of our decision within 90 days.
 1. Each SLO will use his own discretion in this regard.
3. Institute checks with local police, security and intelligence agencies, and SLOs in posts where a previous residence is indicated.
 1. Where no facilities exist in the country of residence, institute Headquarters subversive indices checks.
 2. Where a prior stay in Canada is indicated, institute Headquarters criminal and subversive indices checks.



s.15(1)

s.16(1)

G. 2. b. 5.



A0145227_47-000292

s.15(1)

s.16(1)

G. 2. b. 5. 7. - Forward two forms Imm. 18 to Headquarters Security Screening with a copy to the Director General, Foreign Liaison.

- Do not locally retain completed forms or copies of completed forms Imm. 18.

6. When all records checks and interview results are favorable, notify the local CEIC/VO by returning the form Imm. 8 stamped "No Reportable Traces - Section 19(1)(e), (f) or (g) of the Immigration Act", with the date of the decision and the SLO's signature.

7. When adverse information is discovered, forward to Headquarters Security Screening all relevant information, e.g. form Imm. 8 with your recommendations and the foreign agency's permission to disseminate when applicable.

8. For cases where war crime involvement is suspected, provide the information to:

1. the Director General Security Screening, and

2. the VO with a request to delay the security decision.

9. Submit a request to Headquarters Security Screening [REDACTED] when the provisions of G.I.E. apply.

1. Retain documentation only on those cases where [REDACTED]

2. Ensure a copy of all documentation has been forwarded [REDACTED]

G. 2. b. 10. When a foreign agency requests information obtained during the screening process or it is deemed to be of direct concern to them, state the reasons for the request and forward it to the Director General Security Screening for necessary approvals and preparation of a brief.

11. If Headquarters concludes that the subject may be excludable under the Immigration Act, notify the CEIC/VO.

12. Upon receipt of immigration screening documents from a VO in a post not served by an SLO, forward all documentation to Headquarters Security Screening.

13. Submit "Monthly Statistical Returns" form 2008 to the Director General, Foreign Liaison.

14. On a quarterly basis, tele [REDACTED] to the Director General Security Screening under the appropriate IA file.

1. These telexes are to reach Headquarters Immigration Security Screening by the tenth of the month following the quarter being reported.

15. Notify Headquarters Security Screening of amendments required to the Immigration World Index - Part I.

G. 2. c. Headquarters Records Management

1. Conduct criminal and subversive indices checks on the prospective immigrant and sponsor when applicable.

- G. 2. c. 1. 1. Forward results to Headquarters Security Screening [REDACTED]

NOTE: [REDACTED]

[REDACTED] are not checked.

2. Open files upon request in accordance with G.I.e.
3. Maintain a statistical record of immigration forms processed as directed by Headquarters Security Screening.

G. 2. d. Headquarters Security Screening

1. When documentation, e.g. form Imm. 8, is received directly from CEIC:

1. Ensure it contains sufficient information to permit proper security inquiries and indices checks. Refer to Immigration World Index - Part I.

- If it does not, complete a "Request for Information" form SSF 217 and send it together with the form Imm. 8 to the CEIC submitting office.

2. If all required information is provided, institute all foreign agency checks.

2. When all checks have been completed and ambiguity or contradiction exists, or for reasons of security or fairness to the prospective immigrant, notify the appropriate operational branch that an interview will be requested and ask for comments in relation to the interview of the subject. Upon receipt of this information:

- G. 2. d. 2. 1. For cases originating in Canada, notify the local Canadian Immigration Center (CIC) to summon the subject for interview and provide all relevant information to the regional CSIS office that will be conducting the interview.
2. For cases where subject resides in the U.S.A., provide all relevant material to the Director General, Foreign Liaison.
3. Assess all available information, in consultation with other operations if required, against the provisions of Section 19(1)(e)(f) and (g) of the Immigration Act and notify the originating SLO or VO of the results only.
4. When reviewing reports of Canadian screening interviews, remain alert to External Affairs requirements outlined in the Immigration Manual IC Chapter 1.40.
1. When subject may have information of value, complete a form Imm. 18.
5. Check the two forms Imm. 18 received from SLOs for completeness and relevancy to External Affairs requirements.
6. Forward one form Imm. 18 to the address indicated.
1. Retain one copy of transmitted information on the subject's file.
7. Ensure all necessary approvals as outlined in G.1.b. are obtained:
1. when an SLO requests dissemination of information to a local agency, or

G. 2. d. 7. 2. before disseminating any information to CEIC.

8. Have Records Management open a file when the provisions of G.I.e. apply.

9. If circumstances may warrant the exercise of ministerial or VO discretion, provide CEIC with an assessment taking into account the sensitivity of sources and other operational considerations.

1. In cases of suspected involvement in war crimes consult with the RCMP Federal Policing Branch prior to providing information to CEIC, the SLO or VO.

10. Cases with adverse traces

1. Forward a security assessment to CEIC, containing:

- relevant information on the subject's activities,
- the potential threat to Canada,
- the applicable section of the Immigration Act, and
- a full assessment of sources of information with any caution to be observed to ensure their protection.

G. 2. d. 10. 2. In sponsored cases or when provisions for appeal exist, respond to the request from CEIC by providing the Solicitor General with a comprehensive assessment of the potential security threat and notify whether a certificate, as provided for under the Immigration Act, is to be taken based on the nature of the information or the need to protect sources or methods of operation.

3. When a criminal conviction surfaces, provide CEIC HQ and RCMP "C" Directorate, Imm. and Passport Branch with the information on form F106, containing any caution to be observed to ensure protection of sources.

4. When prior notification of an intent to emigrate is indicated, e.g. sponsored cases, and adverse information exists, alert the SLO or the VO through CEIC HQ and request an interview.

- Provide the SLO with all relevant information including a draft of possible questions, if necessary,

OR

- Provide the VO with relevant information together with a list of possible questions, taking into account the sensitivity of sources and other operational considerations.

G. 2. d. 11. Upon completion of the immigration screening process, forward cases for assessment purposes to:

1. CI(1), CI(2) or Counter Terrorism as applicable, when residence in a Communist bloc country is indicated within three years prior to the date of application;
 2. the appropriate operational branch, when national security factors are present; or
 3. the DCI Attn: Federal Policing Branch when there is any indication of possible involvement in war crimes.
12. Consult with the director general of the appropriate operational branch to have an updated threat assessment and interview material provided. Forward replies to the SLO or to the CSIS Regional Office.
13. Destroy forms Imm. 8 on which no file has been opened.
14. Notify CEIC of amendments required to the Immigration World Index - Part I in accordance with foreign agency requirements.

G. 2. e. Regional Office

1. Conduct all immigration screening interviews in Canada as directed by Headquarters Security Screening utilizing when possible, an investigator with expertise in the subject's area of origin.
2. Hold interviews in CEIC premises making all arrangements locally.

G. 2. e. 3. When an interview of a spouse or a dependent is requested, conduct interviews consecutively and separately from that of the subject.

4. CEIC normally provides an interpreter.

1. For sensitive cases, arrange in advance for a security cleared interpreter.

2. All interpreters must be subject of criminal and Headquarters subversive indices checks.

3. If sensitive information comes to light during an interview and an interpreter without a proper security clearance is present, consider adjourning the interview until a security cleared interpreter is available.

4. Do not use an interpreter who is a friend or relative of the applicant.

5. Identify yourself as a member of the Service and explain that the purpose of the interview is to determine admissibility in accordance with Canadian law.

6. When the subject appears at the interview with counsel:

1. Conduct the interview as planned.

2. Report any interference to Headquarters Security Screening.

7. Ensure you do not create the impression that the subject's suitability for permanent residence in Canada is dependent upon his/her cooperation with the Service or in providing intelligence.

G. 2. e. 8. When information is discovered which is not relevant to Section 19(1)(e)(f) and (g) of the Immigration Act but may lead to discretionary exclusion by the Immigration Officer, e.g. admission to a criminal record, lying, falsification of form Imm. 8, suspicion of involvement in war crimes, consider having an Immigration Officer attend the interview and notify Headquarters Security Screening of the circumstances.

9. Ensure that sensitive sources of information are fully protected.

10. Forward all relevant documentation to Headquarters Security Screening for assessment of subject's security status.

G. 2. f. Director General Operational Branch

1. Upon request provide:

1. a case assessment and advice to Headquarters Security Screening, and

2. ongoing threat assessments and updated interview criteria.

G. 2. g. Foreign Liaison Branch

1. When subject resides in the U.S.A., contact the Immigration Consul at the originating Canadian Consulate to summon the subject for an interview.

2. Conduct an interview in accordance with operational criteria.

G. 2. g. 3. If all records checks and interview results are favorable, notify the Immigration Consul by returning the form Imm. 8 properly stamped, dated and signed as indicated in G.2.b.6.

4. Refer cases for decision to Headquarters Security Screening with all relevant documentation when:

1. adverse information is discovered,
2. information may warrant the exercise of ministerial or consular discretion, or
3. other unusual circumstances are present.

5. When the subject resides in South Africa, Lesotho, Botswana, Swaziland or Zimbabwe, follow the same procedures as in G.2.g.1.

1. Address the request to the immigration officer at the Canadian Embassy in Pretoria, South Africa as these countries fall within the responsibility of that office.

G. 3. Visitor Screening - [REDACTED]

G. 3. a. General

1. The Service is responsible for providing advice to CEIC on non-immigrant visitors to Canada

1. [REDACTED]

G. 3. a. 2. Deadlines for responding to the telex notification from CEIC/VO or External Affairs Posts abroad are as follows, otherwise the visa is automatically issued:

1. five working days for all notifications, and
2. ten working days for [REDACTED]
3. The VO has limited discretion to issue a visa to individuals from countries outlined in Schedules A and B of Appendix II-3-5.
 1. Visas are normally issued to individuals from Schedule C Countries without the usual waiting period however, particulars of the issuance are forwarded to Headquarters Security Screening via diplomatic bag and marked "FOR INFORMATION ONLY".

G. 3. b. Headquarters Records Management

1. Conduct subversive indices check and forward the results to Headquarters Security Screening with all file numbers and related [REDACTED]
2. Open files upon request.
3. Maintain statistical records of [REDACTED] cases processed as directed by Headquarters Security Screening.

G. 3. c. Headquarters Security Screening

1. Ensure all indices checks have been completed.

G. 3. c. 2. If there are possible adverse traces:

1. Notify the VO by message, and inform CEIC HQ to withhold visa until further notice.
 2. Consult with appropriate operational branches and/or foreign agencies.
 3. Assess the information obtained.
 - If traces are assessed nonadverse and no extenuating circumstances exist, notify the VO and CEIC HQ.
 - If traces are adverse, follow the procedures outlined in G.3.c.4.
 4. Provide CEIC with an assessment of relevant information, if circumstances warrant the exercise of ministerial or VO discretion.
3. If there are adverse traces, notify the VO by message and provide CEIC with:
1. an assessment of relevant information on the subject's activities,
 2. the potential threat to Canada,
 3. the applicable section of the Immigration Act, and
 4. a full assessment of sources of information with any caution to be observed to ensure their protection.

G. 3. c. 4. After [REDACTED] procedures are completed, forward files to appropriate operational branch, when:

1. adverse traces exist; or
2. circumstances of operational concern, e.g. visiting VIP, are present.
5. Destroy all [REDACTED] notifications on which no file has been opened.

G. 4. Visitor Screening General

G. 4. a. Counter Intelligence (CI), Subversion (CS) and Terrorism (CT)

1. If it is learned that a person who is adversely recorded in CSIS indices is intending to visit Canada:
 1. Determine if the adverse information could have a bearing on the visitor's admissibility.
 2. Provide the information to the Director General Security Screening.
2. If Counter Terrorism receives adverse information concerning [REDACTED] in Canada or applying to enter Canada and if they may be rejectionable under Section 19(1)(e), (f) or (g) of the Immigration Act, provide the Director General Security Screening with:
 1. a brief prepared according to the information on file, and
 2. a full assessment of organizations/committees the subject is associated with.

G. 4. b. Headquarters Security Screening

1. Provide CEIC Headquarters with any information received from other operational branches on any proposed visitor to Canada when the information could have a bearing on the visitor's admissibility.
1. The information should be provided to CEIC regardless of whether the subject is from a country where no visa is required.

H. SECURITY CLEARANCE OF EXECUTIVES,
OFFICIALS AND EMPLOYEES OF COMPANIES

H. 1. Policy

- H. 1. a. For the purpose of establishing the reliability of a company to enter into a contract or have other dealings of a security nature with [REDACTED]

[REDACTED] the Service shall:

1. financially screen the company or commercial person, and
2. security clear executives, officials and employees of the company who will have access to classified information.

EXCEPTION: In extraordinary circumstances, where the clearance procedure may jeopardize the operation or activity, the DDS on the advice of the DG Internal Security may waive the clearance requirements.

- H. 1. b. Internal Security shall coordinate the conducting of the security clearances and shall ensure the appropriate files are opened to accomodate the clearances.

H. 2. Clearance Procedures

H. 2. a. [REDACTED] Project Officer

1. If there is a need to have a company cleared as required by H.1.a., provide details of the requirement through the Director General [REDACTED] to the Materiel Management Section and request a security clearance.

1. Indicate the level of security clearance required.


H. 2. b. Director General [REDACTED]

1. Ensure the [REDACTED] need for outside personnel is justified.
2. If the security clearance is refused and you feel the [REDACTED] need clearly outweighs the requirement for a security clearance, provide the details to the DDS.

H. 2. c. Materiel Management Section (MMS)

1. Upon receipt of a request to have a company or commercial person cleared, determine:
 1. whether the company has been previously cleared, and
 2. if the security clearance is still valid.
2. If the company or commercial person has a current security clearance, proceed as indicated in H.2.c.6. and 7.

H. 2. c. 3. If the company or commercial person has not been previously cleared, obtain the necessary biographical data for the individuals involved on a:

1. Personal History Form (PHF),
 2. Security Screening Form 1981,
 3. Company application form, or
 4. Other media, eg personal resumé.
4. When deemed appropriate, ensure fingerprints are taken of those persons to be cleared.
5. Provide the information obtained from the company to Internal Security and request the appropriate security clearance be conducted.
1. Inform Internal Security of the mode of contracting, e.g.

6. Administer the Oath of Secrecy to the company representatives cleared and document the oath on the appropriate forms or file.
7. When required, request Internal Security to cancel, upgrade or update a security clearance.

H. 2. d. Internal Security

1. Upon receipt of a request for a security clearance related to a company or commercial person:

1. Ensure the appropriate file is opened to accomodate the clearance,
2. Check with [REDACTED] to determine if the company is listed with Supply and Services Canada (SSC),
3. Ensure an [REDACTED] financial investigation of the company is conducted and forwarded to MMS for an assessment.
4. Request Headquarters Security Screening to conduct the necessary checks.

2. If it is determined a security clearance should be granted, provide the DG [REDACTED] and MMS with a Certificate of Security Clearance.

1. If a security clearance cannot be issued, provide the reasons in writing to the DG [REDACTED] and MMS.

H. 2. e. Headquarters Security Screening

1. Upon request from Internal Security, conduct the appropriate checks and notify Internal Security of the results.