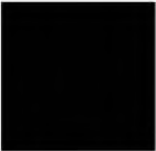



s.24(1)

GOVERNMENT SECURITY SCREENING
PROCEDURES

A. REFERENCES

1. Charter of Rights and Freedoms
2. CSIS Act
3. Access to Information Act
4. Privacy Act
5. Criminal Records Act
6. Young Offenders Act
7. Government Security Policy and Personnel Screening Standards
8. Operations Manual - II.3 (Security Screening)
9. Operations Manual - II.4, II.6
10. Ministerial Directives, 1986, 1989
11. Security Screening Branch Annual Plan
12. MOU Between CSIS and DEA
13. MOU Between CSIS and DND
14. MOU Between CSIS and RCMP
15. International Industrial Agreement
- ✓ 16. Public Service Employment Act
17. Financial Administration Act
18. Canadian Human Rights Act
19. Government Security Screening Policy

 This is only the 2nd Draft of an update
to our procedures Manual. I've copied
some pages I thought you might be
interested in.

 90.05.11

A0140227_1-001316

B. PROCESS AND DECISIONS - GENERAL

*all sub titles
should be in
bold print.*

B.1. Initial Processing Steps

Security assessment requests from government departmental security offices and allied agencies are directed to the Security Screening [REDACTED] Unit of Records management Branch. SSSU personnel are responsible for opening the appropriate security screening file and conducting an initial quality control check of the GSP documentation received concerning a security clearance candidate. The Unit will also forward the candidate's fingerprints to the RCMP for processing and conduct CSIS indices and credit bureau checks. Depending on the result of the CSIS indices check, [REDACTED] may be sent to the [REDACTED] Unit where a decision is rendered as to whether the candidate [REDACTED]

The results of these checks and all relevant material is sent to the Security Screening Branch for further processing and security assessment evaluation.

- B.1.2. Security Screening files received by the Branch are initially stored by the [REDACTED] Unit, where they are sorted according to priority and portfolio unit designation. With the exception of Level 1 security clearance requests, which can be processed on the basis of a Criminal Name check only, all files must await the results of the RCMP fingerprint check before further security assessment consideration can take place.

B.2. Secondary Processing Steps

A security assessment is required in all cases where a person's duties or tasks require access to classified information or assets, or access to essential persons or installations critical to the national interest. The attached chart outlines the process to be followed and the decisions to be made in the conduct of a government security clearance investigation. This process may consist of up to twelve steps in order to produce a

security assessment to a federal government institution. Security assessments contain the results of our investigation and a recommendation concerning whether an individual should be granted or denied a security clearance.

B.3. Decision on Security Relevance

The first decision point requires the analyst to review the results of all indices checks and decide whether to respond with a positive assessment for Level 1 and 2 requests, or proceed further because of questions raised by the indices checks or because a Level 3 field investigation is required.

B.4. Evaluation of Initial Indices Checks

The analyst must carefully evaluate all available information which could or might affect a deputy head's decision concerning an individual's security clearance status [REDACTED]

[REDACTED] The analyst must decide, based on the nature of the information, whether to ignore the information as not being of security concern, and prepare a standard security assessment in the case of a Level 1 or 2 clearance, or to institute an investigative action.

B.5. Investigative Options

The seriousness of the information must be considered by the analyst in selecting the investigative options available. Basically the options are a subject interview, full field investigation, partial field investigation, or a combination of the aforementioned. Also, it may be necessary to request an assessment [REDACTED]

[REDACTED] identifying any security concerns presented by the section 12 CSIS Act trace information. If there is a requirement to task an allied service because the subject (or relatives in some cases) has lived abroad for a year or more, the analyst will prepare a request for the appropriate out-of-country check(s).

B.6. Decision on Tasking

The analyst must now decide on the tasking to be requested of the field or allied service. See attached sheet for insert. The information available will suggest certain questions that must be addressed in order that sufficient information is obtained to complete a proper security assessment. Specifically, the field is to be tasked to carry out an enquiry which not only addresses the standard GSP questions concerning loyalty and reliability but which also requires the investigator to delve into the specific issues surfaced by the information available. In doing this, the analyst may prepare very specific questions to be asked and identify specific individuals to be questioned. If the individual is being considered for a Level 3 security clearance, the analyst will task Security Screening field offices in all Regions where the candidate has resided [REDACTED]. If issues of potential security concern are present, the analyst must also focus the investigation on those concerns to ensure that the Service is in a position to provide a thoroughly complete security assessment and well considered security clearance recommendation. ✓

B.7. Evaluation of Field Reports

When the field enquiries have been completed and the results received, they must be evaluated by the analyst in relation to GSP requirements and established Branch criteria (i.e. loyalty and related reliability, time and source coverage). The analyst must ensure that all security concerns have been fully addressed and that the thoroughness of the investigation has not been jeopardized by such things as open ended statements that require further resolution (i.e. "The subject no longer uses drugs"). The analyst must also ensure that specific issues previously identified to the field as being of possible security concern have been addressed to the fullest extent possible. In summary, there are five general criteria by which all reports are evaluated:

- (a) Have all aspects of GSP been thoroughly covered (i.e. standard questions on loyalty and reliability)?

- (b) Have all specific questions, especially on security concerns, been fully answered?
- (c) Has any potentially derogatory information concerning the clearance candidate been corroborated through additional enquiries?
- (d) Is there adequate source coverage [REDACTED]
- (e) Is the required time period covered, [REDACTED]

B.8. Decision on Relevance and Sufficiency

The analyst must then assess all the information gathered and decide on its relevance and sufficiency ensuring the report(s) meets the required criteria. In many cases there will be no adverse information which will indicate a favourable reply to the responsible federal institution. However, there may be information that reflects on the subject's loyalty or reliability as it relates thereto. This may vary from section 12 CSIS Act trace information on the subject and/or relatives to "features of character" such as abuse of alcohol/drugs, financial problems, criminal behaviour, etc. If the analyst determines that the investigation is deficient in coverage, the analyst must address *by re-tasking* this concern ~~to~~ the field in order to rectify the problem. In some cases this may entail directing the field to conduct a security interview with the subject to resolve outstanding security concerns. When the analyst is satisfied that the investigation is as complete as possible he/she makes a judgement on what is, or is not significant, recommends the appropriate action, and prepares an initial assessment.

B.9. Summation and Initial Conclusion

The analyst prepares a short summary of the relevant security information and background of the case. On the basis of the information available he/she then prepares a recommendation ~~to~~ *whether* ~~suggest that~~ ^{she/he} the person be granted or denied a security clearance. The recommendation and all relevant documentation is then forwarded to [REDACTED]

B.10. Review and Evaluation

The [redacted] analyst reviews the complete file and makes a similar evaluation of the case. *If* ~~In the event that~~ the [redacted] analyst is not satisfied with some aspect of the investigation he/she outlines these concerns to the Screening analyst who would then re-task the field to address the concern, and permit further enquiries for the gathering of additional information considered essential.

B.11. Decision on Reporting

When the [redacted] analyst is satisfied that the investigation is complete he/she must then assess the available information to determine what information should be reported to the Departmental Security Officer (DSO) or Deputy Minister of the responsible federal institution in order that a sound decision can be made on whether to grant or deny a security clearance.

B.12. Preparation of the Security Assessment

The [redacted] analyst then prepares a detailed security assessment which identifies what was done, comments on the loyalty and reliability of the subject, and then makes a recommendation regarding the granting of a clearance to the subject concerned. The assessment must be based on all available information, favourable or unfavourable, and must not reflect the [redacted] analyst's personal preferences.

B.13. [redacted] ^{analyst} reviews each assessment to ensure consistency in quality and in support documentation. The assessment can be sent back for re-write by the [redacted] or the file back for further tasking of the field if required. The final decision on all favourable screening requests that involve field enquiries is made by [redacted] Unit in consultation with DDG when required. If a recommendation for denial is considered, the agreement of the DDG-FSS, DG-FSS, DDF, Legal Services and the Director is required.

B.14. Sign-off to Requesting Department

The final detailed security assessment is then produced by the Branch's [redacted] Section and signed off to the requesting federal institution.

E. FIELD TASKING AND INVESTIGATIONS - GENERAL

E.1. GENERAL

- E.1.1. In accordance with the GSP, a full field investigation is required for Level 3 clearances. In cases of Level 1 and 2, however, an investigation will normally be conducted "for cause". Similarly, special situations or events may dictate to undertake an investigation.
- E.1.2. The investigational and analytical components of the security screening process is crucial for the quality of assessment of a person's loyalty and related reliability. It is, therefore, highly important that vigilance and precision be attained. Employees involved in the process should be well acquainted with the Guide to Field Investigators and Headquarters Analysts.

E.2. Headquarters Analysts

- E.2.1. In tasking the field to conduct and investigation "for cause" you may elect to use one or more of the following options:
- (a) Subject interview;
 - (b) full field investigation;
 - (c) partial field investigation;
 - (d) any other checks you believe to be necessary for the purpose of making a complete and objective security assessment (Note: prior to initiating these checks authorization must be received from DDG-FSS).
- E.2.2. Specify to regional office the type of investigation i.e., clearance to Level 3 (10 or 20 years) or Level 1 or 2 "for cause".
- Provide:
- (a) A copy of the Personnel Security Clearance Questionnaire for the candidate together with a legibly completed signed Consent form (TBS/SCT 330/58);
 - (b) any trace information including [redacted] check results, if the investigation is "for cause";
 - (c) the results of credit bureau checks(s), including Service 12;
 - (d) any criminal record traces;

- (e) any specific investigational instructions;
- (f) the name, if any, of other regional offices involved in the investigation;
- (g) a diary date; and
- (h) in the absence of relevant information surfaced by the checks enumerated above, so inform the Region(s).

Use the appropriate screening file to correspond when the investigation is to clarify [REDACTED] or to determine influence factors.

- E.2.3. When enquiries are being conducted by more than one Region and a potential security concern surfaces, this should be transmitted without delay to all concerned investigating Regions.

Note: Request Regions to refer all questions in respect to policy, procedures or matters pertaining to the investigation which need clarification to headquarters.

- E.2.4. When a report is received from the regional office, review it for thoroughness, objectivity and relevance and ensure every reasonable effort has been made:

- (a) to corroborate or refute both positive or derogatory information;
- (b) to ensure identification;
- (c) to resolve any doubt;
- (d) to clarify [REDACTED] and
- (e) to properly assess the information provided by all sources.

If a report is considered inadequate, provide appropriate direction to the Regional Office.

- E.2.5. When information indicates a security clearance may be denied, withdrawn or downgraded, request an interview of the subject:

- (a) to confirm or refute the allegations;
- (b) to allow the subject to explain and put the information in proper context; and
- (c) to allow the investigator to assess the veracity of the subject.

NOTE: [REDACTED]

EXCEPTION: For RCMP and DND (See chapter)

E.3. Investigator

E.3.1. Carefully review the candidate's PSCQ as well as any related documentation and establish a plan of action.

E.3.2. When practical, consult telephone or city directories or similar publications to verify addresses and establish possible source of information.

E.3.3. [REDACTED]

E.3.4 Conduct a check of local police records on the subject.

E.3.5. When making inquiries, consider the following sources of information:

E.3.6. To the fullest extent possible, interview only respected, responsible members of the community who have personal knowledge of the subject of inquiry.

- E.3.7. Make every effort by telephone to arrange appointments for interviews with sources and:
- (a) 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.
 - (b) Establish whether the source knows the candidate well enough to assist the investigation.

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

- E.3.8. 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.
- E.3.9. Attempt to put the person being interviewed at ease and keep questions brief, uncomplicated and unthreatening. Make full use of follow-up questions to elicit full details about the candidates behaviour, loyalty to Canada and related reliability.
- E.3.10. During the interview, take precautions to ensure all sources, methods of operations and targets are protected to the fullest extent possible.
- E.3.11. 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, (i.e. sexual behaviour, venality, alcoholism, debt, or gambling) are conducted with sensitivity, tact, discretion, maturity of judgement and the absence of bias.

NOTE: The behaviour of an individual, including a person's sexual orientation, may be of consequence in a security clearance context if that behaviour could or might leave the individual vulnerable to blackmail, coercion or to be indiscreet and untrustworthy with classified government

information and assets. But, without information suggesting the individual behaviour represents a security risk, it is the Service's position that a person's sexual orientation is not in and by itself a security risk.

- E.3.12. Ask source for specific examples of why the candidate is or might be 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.

- E.3.13. 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.

- E.3.14. When adverse information surfaces during an inquiry, attempt, to the fullest extent possible, to corroborate it.

- E.3.15. Explore fully how the candidate copes with an alternate lifestyle emphasizing whether he or she is embarrassed or secretive about it and if vulnerable to compromise, blackmail or indiscretion.

- E.3.16. 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.

NOTE: Prior to initiating any of the above avenues of investigation, authorization must be obtain from Headquarters.

- E.3.17. When making inquiries or conducting an interview, explore:



E.3.18.

E.3.19.

E.3.20.

E.3.21.

E.3.22.

E.3.23.

E.3.24.

E.3.25.

E.3.26.

E.3.27.

E.3.28.

E.3.29.

E.3.30.

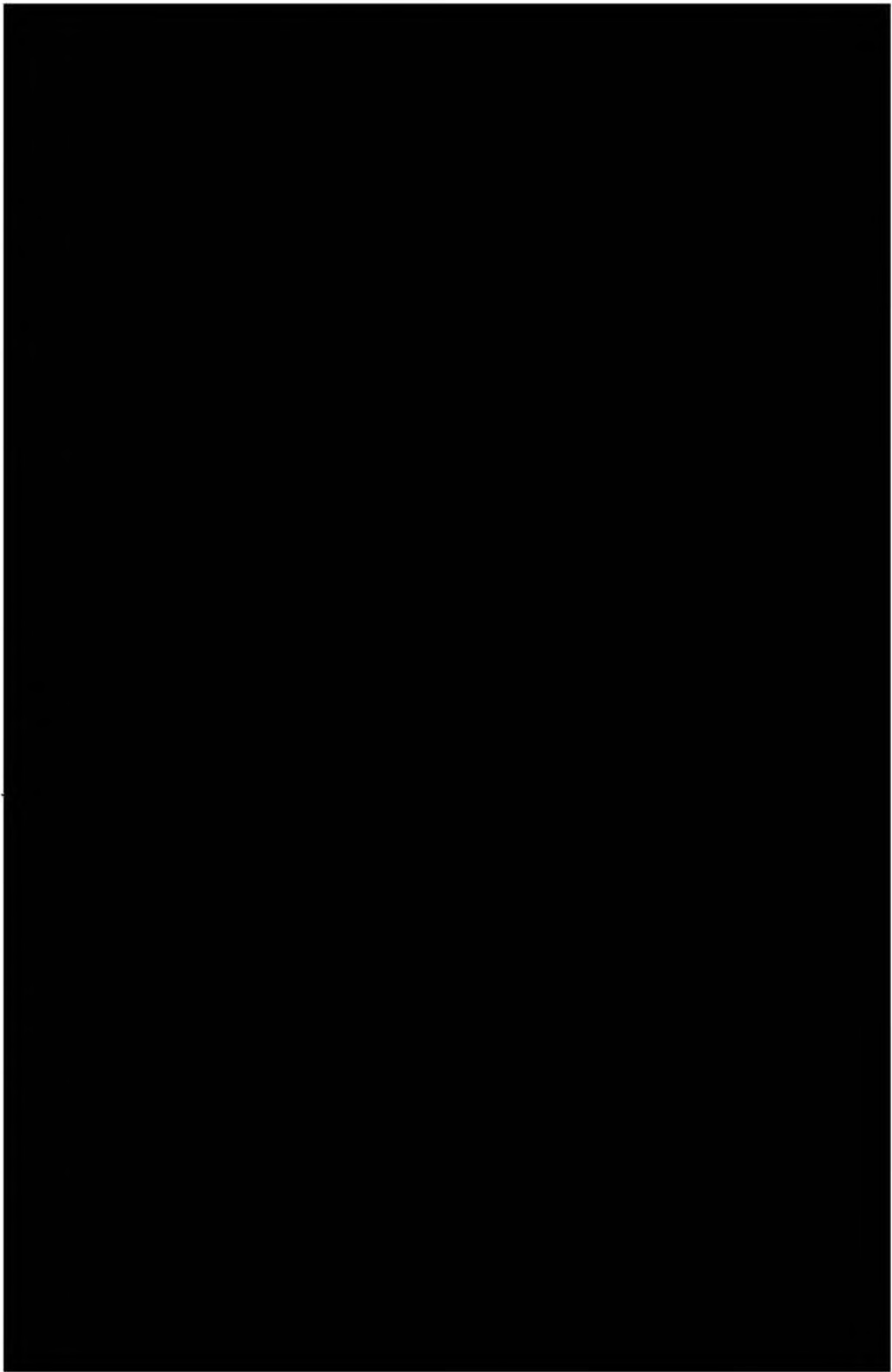
E.3.31.

E.3.32.

E.3.33.

E.3.34.

E.3.35.



E.3.36.

E.3.37.

E.3.38.

E.3.39.

E.4. Reporting

E.4.1. Report all information developed which is relevant to determining whether a candidate should be given a security clearance.

NOTE: When the investigation is for an employee of the CSIS, 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.

E.4.2. 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.

- E.4.3. When you do not know whether or not to believe the comments of a sources, indicate in your report that the information is unverified and is being reported without any assessment as to its reliability.
- E.4.4. Avoid any subjective comments regarding whether the candidate should be afforded access to classified material.
- (a) 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.
- E.4.5. Provide a full assessment of all sources used in the investigation and include:
- (a) their relationship to the candidate, i.e. social, coworker, recreational or casual;
(b) the apparent knowledge of the candidate over what period of time;
(c) any indication of dishonesty or bias in reporting for or against the candidate;
(d) the basis for any belief or opinion expressed; and
(e) the expectation of confidentiality as provided for in the Privacy Act.
- E.4.6. When the subject is an employee of or a candidate for CSIS, a separate suitability report should be submitted to the DG - Personnel Services.