

FOR RCMP EYES ONLY

(DRAFT 23)

F. Government Screening - Federal Institutions

F. 1. Policy

- F. 1. a. Only personal information relevant to the suitability of an individual for access to assets classified in the national interest shall be collected or disclosed to a government institution in which case disclosure shall be to the Departmental Security Officer (DSO) or to the Head of Institution when the DSO is subject of inquiry.
- F. 1. b. Security clearance procedures shall not be carried out on behalf of any individual, company, police force, provincial or municipal government except through a Federal Government institution.
- F. 1. c. Where any doubt exists as to the level or the propriety of a request for a security clearance, the institution shall be challenged to justify the inquiry under C.D. 35.
- F. 1. d. Information that subject does or may advocate separatism shall not be collected but shall be reported if it is available.

F. 1. e. Sources who admit homosexual activity shall not be reported on or made subject of a file on the basis of that admission alone.

F. 2. General

F. 2. a. The Security Service is responsible for providing a security assessment of the loyalty to Canada and the reliability as it relates thereto of candidates for, or incumbents of, positions in federal government institutions listed in schedules A-D of the Financial Administration Act, or persons involved in classified defense related work for such institutions, or persons having custodial responsibility for classified assets in areas vital to the national security, or persons charged with the security of facilities where such classified assets are retained.

F. 2. b. A security clearance may be requested for:

1. employees of the federal government with access to assets classified in the national interest or with custodial responsibility for such assets.
2. employees of provincial or municipal governments with access to such federal government assets.

3. persons in the private sector involved in, or engaged upon the production or study of classified defense equipment.
4. persons, who are not intended to have access to classified assets, but who, due to their work environment may have unintended access, or where such unintended access is a reasonable apprehension.
5. members of the Cabinet and parliamentary secretaries.
6. order-in-council appointees of the federal government.
7. Ministers' exempt staff.
8. Employees of companies who will be involved with contracts of a classified nature with the Security Service per SSOM 65.

F. 3. Standards of security clearance

F. 3. a. Confidential and Secret - based on a check of:

1. fingerprints and subversive indices, and
2. foreign agency indices, as required, or

3. field investigation for cause.

F. 3. b. Top Secret - based on a check of:

1. fingerprints and subversive indices, and
2. credit bureau records.
3. a field investigation covering the immediately preceding 10 year period, or to 18th birthday.
4. foreign agency indices when required, including field inquiries.

F. 3. c. Special Activity (S.A.) - based on a check of:

1. fingerprints and subversive indices.
2. local law enforcement agency records in vicinity where the individual has resided for substantial periods of time.
3. credit bureau records.
4. a field investigation covering the immediately preceding 20 year period, or to 18th birthday.

5. foreign agency indices as required, including field inquiries.

F. 3. d. Security Panel (SP)243 (Applies to Canadian Corps of Commissionaires employed in the National Capital Region)
- based on a check of:

1. fingerprints and subversive indices,

2. credit bureau records,

3. a field investigation covering the immediate preceding three years, excluding Department of National Defence and Canadian Corps of Commissionaires employment.

4. foreign agency indices as required.

F. 3. e. Cursory - based on a check of:

1. subversive and criminal indices on the basis of information supplied.

F. 4. Screening

F. 4. a. Follow the procedures outlined in App. II-3-4.

F. 5. Criminal Records

F. 5. a. Policy

1. No criminal record which has been subject of a pardon shall be disclosed without the consent of the Solicitor General.
2. A criminal record shall not be reported as fact to a DSO unless it has been confirmed by a comparison of fingerprints.

. 5. b. General

1. A check of the criminal record is normally performed on the basis of fingerprints submitted directly to "I" Directorate by the responsible DSO. "I" Directorate will provide the result directly to the DSO and only consult "A" Operations when:
 1. a pardoned criminal record is involved.
 2. a criminal record develops on a person whom "I" Directorate believe to be employed by the Federal Government.

3. a warrant is outstanding.

F. 5. c. "A" Ops. - Screening Unit

1. When criminal record has been pardoned, but is judged directly relevant to security:

1. Seek Ministerial waiver through "I" Directorate, as provided for in Section 6(2) of the Criminal Records Act.

2. Hold report to LSO in abeyance pending decision as to whether record may be disclosed.

3. Notify the DSO that a reply will be delayed.

4. Return pardoned criminal record to "I" Directorate when it is judged NOT RELEVANT TO SECURITY STATUS, or where no Ministerial Waiver has been obtained, and retain no copy or record.

5. When it is deemed necessary to maintain some record of a pardoned criminal offense, request "F" Operations to seal record on file to be opened only by the CIC "F" Ops.

2. When a criminal record is discovered on a subject of a security screening inquiry:

1. Obtain all relevant information from "I" Directorate.
2. Determine whether the record has been the subject of a pardon.
3. Together with the [REDACTED] Unit assess the full relevance of the record including the circumstances of intended employment when:
 1. the record has been pardoned,
 2. an absolute discharge has been registered,
 3. a criminal investigation did not lead to charges being laid, and
 4. a warrant is outstanding.

3. When "I" Directorate advise of a criminal record believed to pertain to an employee of the Federal Government:

1. determine from the responsible DSO, if the person is

employed in a position falling within the ambit of
F.2.B.

2. only in cases where access is confirmed, advise the
ESO that he should update his security record by
forwarding fingerprints to "I" Directorate,
Identification Services, Civil Section.

4. When a warrant is determined to be outstanding on a person
requiring a security clearance:

1. Contact the warrant holding agency through Security
Service liaison channels on an urgent basis to
determine:

1. if the subject of inquiry is identical to the
person named in the warrant.

2. the circumstances of offence in respect
of which the warrant was issued.

3. what action has been taken, or is intended
to be taken, to execute the warrant.

2. Forward to [REDACTED] Unit for notification of the DSO.

3. When no fingerprints have been submitted to "I" Dir. and warrant is returnable, notify the DCI in writing.

F. 5. d. "I" Directorate

1. Upon receipt of fingerprints, conduct a criminal name index check of GPIC and a complete fingerprint search for a criminal record.
2. Report results to D.S.O.
3. Advise "A" Operations in accordance with F. 5. b. 1.

F. 6. Foreign Agency Checks

F. 6. a. Policy

1. Only information necessary to permit a proper inquiry shall be disclosed when checking with an approved foreign agency.

F. 6. 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 conditions. These are described in the Immigration World Index - Part I.

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. spouse.
3. on persons who have resided outside Canada for a period in excess of one year in a capacity other than as an employee of a Federal or Provincial Government.
4. to resolve doubt or to clarify traces.
5. as otherwise specifically requested by the DSO.

F. 6. c. "A" Ops.

1. Request action through LO or directly from agency in the case of [REDACTED]
2. Advise DSO of time required before a reply from a foreign agency can be expected.
3. Provide to foreign agency only as much personal

information about the subject as is necessary to permit proper inquiries.

4. Provide DSO with revised time estimates when checks exceed the original estimate.

F. 7. Credit Bureau

F. 7. a. Policy

1. All searches of credit bureau records on behalf of government institutions other than the RCMP shall be conducted by "A" Operations HQ and in writing.
2. All user fee charges shall be verified monthly against a log of security screening cases maintained for that purpose.
3. No information obtained as a result of a search of credit bureau records shall be disclosed except for purposes of employment or otherwise provided for in the Privacy Act.

F. 7. b. General

1. In accordance with C.D. 35, the Security Service is responsible for conducting a check of credit bureau

records in respect to all requests for Top Secret security clearances or as otherwise deemed necessary to ensure the subject of inquiry is one in whom the Federal Government may repose full trust and confidence. The Force also conducts Credit Bureau checks in respect to the employment suitability of its own members in accordance with A.M. XI.2.

F. 7. c. "A" Ops. Screening Analyst

1. Conduct a check of credit bureau records at the location of the most recent address shown on the Personal History Form or as otherwise deemed advisable.
2. Complete, sign and forward Service Request Coupon to "A" Ops. Admin. Clerk.
3. On receipt of the credit bureau report, submit to the Admin. clerk for logging and forward details to Area Commands involved in the investigations.
4. When investigation is complete and assessment has been forwarded, seal credit information to be placed on file to be opened only by supervisors of "A" Ops. screening or [REDACTED] unit.

F. 7. d. "A" Ops. Admin. Clerk

1. Log the credit bureau request and forward by mail to the appropriate Credit Bureau.
2. Log the credit bureau report and forward to screening analyst.
3. Verify credit bureau report invoice with log at end of each month and bring irregularities to attention of supervisor.
4. Have the credit bureau invoice certified by supervisor and forward to F.S.S.

F. 7. e. H.Q. F.S.S.

1. Ensure invoice has been properly certified.
2. Remit payment.

. 7. f. Investigator

1. If you believe that relevant information having a direct bearing on your investigation is available at a local credit bureau office which is not being contacted by

headquarters, request headquarters to conduct a check of the credit bureau records in your area.

F. 7. g. Area Command "F" Ops.

1. Seal all credit bureau information on file to be opened only by supervisor of security screening unit.

F. 8. Curscry Records Check - Cabinet Appointees and Parliamentary Secretaries

F. 8. a. Policy

1. The RCMP shall only respond to requests for screening received from the Secretary to the Cabinet or his designate.
2. The Security Service shall be responsible for:
 1. co-ordination of indices checks, and
 2. preparation of a report detailing and assessing information of a subversive or criminal nature that may affect an appointment.

3. All requests shall be processed urgently on a strictly need-to-know basis. .

F. 8. b. General

1. The RCMP may be requested to conduct cursory subversive and criminal record checks, under authority of Cabinet Directive 35, of:

1. appointees to the Cabinet, and
2. Parliamentary Secretary appointees.

2. Results are given to the Secretary to the Cabinet by the Commissioner.

F. 8. c. CIC "A" Operations

1. Obtain all pertinent data concerning the appointee - consult the Canadian Parliamentary Guide if necessary.
2. Provide available biographical information to the DCI, in writing.
 1. Request an urgent criminal records check including

details of any ongoing criminal investigation in which the nominee/appointee or his/her spouse may be implicated.

3. Initiate a subversive indices check on a priority basis.
 1. Where loyalty traces are surfaced, ensure that a check of "L" Ops indices is made.
4. Assess all relevant security traces and compile a summary.
5. Qualify the information when:
 1. time does not permit full checks, or
 2. lack of biographical data does not permit positive identification.
6. Do not initiate investigative action unless instructed by the Director General.
7. Prepare a report combining security and criminal assessments and forward it through the Director General to the Commissioner.
8. Deliver file to the D.G. for a determination as to

restriction of access.

F. 8. d. CIC "F" Operations

1. Conduct records check upon request from "A" Operations.
2. Open [REDACTED] category file for each subject of security screening notwithstanding that another operational category file may exist.
3. Ensure future access to these files is restricted as directed by the D.C.

F. 8. e. ICI

1. Refer the request to National Crime Intelligence Branch for processing as follows:
 1. Conduct name checks of:
 1. criminal record indices (CPIC)
 2. the Automated Criminal Information Intelligence System; and
 3. files retained by Headquarters

Operational Records Section.

2. Refer the request by priority classified message to divisions with which the subject is associated because of birth, residence, employment, etc. and request a name check of operational files, down to the unit level.
3. If there is no trace, prepare a negative response for signature of D.C.I.
4. If a name check appears positive, forward the request to the appropriate "C" Directorate policy centre to fully research the matter and prepare the "C" Directorate response.
1. Stipulate that the information is being provided in confidence and is only to be used for the purpose it was requested.
2. Quality the information if:
 1. it cannot be fully substantiated.
 2. the search was adversely affected by the lack of complete identifying data.

3. State that the name checks do not include searches of:

1. information collected and held by other police departments, or

2. records or investigations of other federal or provincial government departments.

2. Review and sign the criminal assessment response (if any) and forward it to the OIC "A" Operations.

F. 8. f. "C" Directorate Policy Center

1. Research and assess any positive criminal record check.

2. Prepare a response for signature by the DCI. See F. 8. f. 4.

F. 9. Cursory Record check - Order-in-Council appointment or Ministers' exempt staff:


F. 9. 1. Policy

1. Personal information shall only be disclosed in response

to a request for a cursory records check pertaining to an Order-in-Council appointment or Ministers' exempt staff when confirmation has been received that the candidate will have access to assets classified in the national interest and a signed PHF has been received.

2. All screening procedures in respect to Order-in-Council Appointees or Ministers' exempt staff shall be conducted on a priority basis.

F. 9. 2. General

1. The intent of the cursory records check in respect to Order-in-Council appointment or Ministers' exempt staff is to assist the government in making appointments at the most senior levels.
- 

. 9. 3. "A" Operations

1. Obtain all available information from the DSO and conduct on an urgent basis.

1. subversive indices check, including a check of "L" Ops. indices, where a loyalty trace surfaces during the subversive indices check.
 2. a CPIC check.
-
2. If no reportable traces are surfaced, advise the DSO that: "Based on the information supplied there are no reportable traces" and note this on the individual's file, or if no file exists, on the general cursory checks file.
 3. If adverse information is present, confirm with DSO that the proposed appointee is to be placed in a position requiring access to assets classified in the national interest and request an up-to-date PHF and submission of fingerprints to "I" Dir.
-
1. upon receipt open [REDACTED] category file,
 2. follow standard screening procedure on a priority basis.
 4. If a security clearance is not a requirement, bring the matter to the attention of the IG and advise the DSO that this is being done.

F. 10. Field Investigation

F. 10. a. Policy

1. In all cases where investigative action is required, the candidate shall be subject of a [REDACTED] category file and no information unrelated to the screening process is to be carried on that file.
2. Where the subject of an inquiry has not resided in Canada for a period permitting reliable inquiries, the subject and his references shall be interviewed to establish positive evidence that his/her first loyalty is to Canada.
3. Local RCMP detachments shall conduct security screening investigations in locations where, in the judgement of the Area Commander, it is impractical for Security Service units to do so.
4. Only experienced, mature investigators shall be employed on security screening duties.
5. Every precaution shall be taken during the course of inquiries to ensure that the individual described by sources is identical to the subject of the PHF.

6. Every effort shall be made to interview responsible, respected members of the community and to corroborate all adverse information developed.
7. Information relating to a subject's character or life style shall not be collected unless it relates directly to:
 1. security screening pursuant to C.D. 35 or,
 2. an operating program of the Security Service.
8. Where adverse information has been developed, the subject of the inquiry shall be interviewed wherever possible having due regard to the sensitivity of sources and other operational considerations.
9. No investigation shall be undertaken to collect or expand upon information involving allegations or suspicion of separatist activity.

F. 10. b. General

1. Indications of fundamental disloyalty to Canada, e.g. involvement in espionage, terrorism, subversive

organizations, will in most cases be discoverable through the search of subversive indices. While questions relating to subversive activity cannot be ignored, the primary value of the field investigation is in determining whether a person's character or life style is such as to lead the subject into indiscretion, dishonesty or render him/her vulnerable to compromise or blackmail.

2. While IND and RCMP normally conduct their own field investigations, any designated Federal government institution may request a field investigation:
 1. in respect to persons being cleared for access to the level of Top Secret.
 2. for members of the Canadian Corps of Commissionaires employed in the National Capital Region.
 3. in respect to persons who are employed in areas vital to the national security where unintended access is a reasonable apprehension.
 4. to resolve doubt in accordance with para. 15 of C.D. 35.
 5. clarify traces.

6. as otherwise deemed appropriate by the T.S.O.
3. While nothing precludes inquiries to the extent necessary to fully resolve doubt, clarify traces, or as deemed advisable by the DSO, field investigations normally do not go back beyond the subject's 18th birthday and cover:
 1. a period of 10 years.
 2. a period of 20 years for persons intended to have Special Activity (S.A.) access.
 3. a period of 3 years for members of the Canadian Corps of Commissionaires in the National Capital Region.
 4. a period of 10 years for members of the Canadian Corps of Commissionaires with access to the level of Top Secret is requested by the employing institutions.
4. The relevance of aspects of character or life style to security can only be judged in their full contextual circumstances. Investigations and reporting, therefore, must go beyond the simple identification of a character trait and provide as full an appreciation as possible of

how the subject copes.

F. 10. c. "A" Operations

1. Conduct credit bureau and CPIC checks.
2. Specify to the Area Command the type of investigation, e.g. SP-243, S.A. standard, FOR CAUSE, and provide:
 1. the PHF,
 2. trace information,
 3. credit bureau results as soon as known,
 4. criminal record as soon as known,
 5. any specific investigational instructions,
 6. diary date, and
 7. the name of other Area Commands involved in the investigation.
3. Correspond on operational file, when investigation is to clarify subversive traces or to determine influence

factors.

4. Correspond on [REDACTED] file, when investigation is to clarify reliability as it relates to loyalty.
5. If the DSO requests a field investigation to clarify allegations or suspicion of involvement in separatist activity, advise him that such investigations are not mandated and take no further action.
6. When the subject of investigation is a person described in F. 10. a. 2. instruct Area Command to interview references and subject, focusing upon the development of positive evidence that the subject's first loyalty is to Canada.
7. When subject of investigation is an employee of, or candidate for, the Security Service, ask Area Commands to remain alert to employment suitability factors.
8. When diary date has not been complied with, request immediate report from Area Command.
9. Review field report for thoroughness, objectivity and relevance and ensure that every reasonable effort has been made to corroborate adverse information, to ensure

identification, to resolve doubt, and that all sources have been assessed. If report is deemed inadequate, provide appropriate direction to Area Command.

F. 10. d. Area Commander

1. Assign only mature, experienced investigators to security screening inquiries.
2. When it is impractical to conduct security screening inquiries with Security Service personnel, forward all information pertinent to the investigations to the RCMP Detachment at the point of inquiry and assign diary date.
3. Have all inquiries necessary to clarify or amplify subversive traces conducted by an investigator with specific expertise.
4. Maintain a statistical record of security screening investigations conducted as directed by HQ - "A" Operations.
5. Conduct only security screening investigations directed by HQ - "A" Operations.

6. Ensure a consistent standard of quality and responsiveness to diary dates.
7. Maintain a program of liaison as you deem necessary with:
 1. Regional security officers.
 2. Security officers in private defense contracting industry.
 3. RCMP Detachments and local law enforcement agencies.

F. 10. e. RCMP Detachment Commander

1. Conduct all inquiries within the time limit allotted by the Security Service area/district commander.
2. Submit the original and one copy of the report and related correspondence on form C-237 to the originating area/district command.
3. Retain one copy of all material for two months from the date of the concluding report then forward to the originating area/district command.

F. 10. f. Area Command - "F" Operations

1. Place the area command copy of the report and all related documentation on file.

1. EF the file to ensure correspondence is returned in compliance with F. 10. e. 1.

2. Retain file in accordance with "F" Operations retention criteria.

F. 10. g. Investigator

The following are guidelines only and not every element will be present in every case. Common sense is still the best guide to uncovering relevant information during a field investigation.

1. Preparation:

1. Carefully review PHF and related documentation and establish a plan of action.

2. When practical, consult telephone book, city directory, etc. to verify addresses and establish possible sources of information.

3. When practical, [REDACTED]
[REDACTED]

4. Make every effort to arrange appointments for interviews by telephone in advance.

1. Describe nature of inquiry.

2. Establish whether source knows subject well enough to assist investigation.

3. Establish a time convenient to the source for a meeting.

4. Avoid conducting any part of the interview by telephone.

5. [REDACTED]

6. Conduct a check of other local police records when:

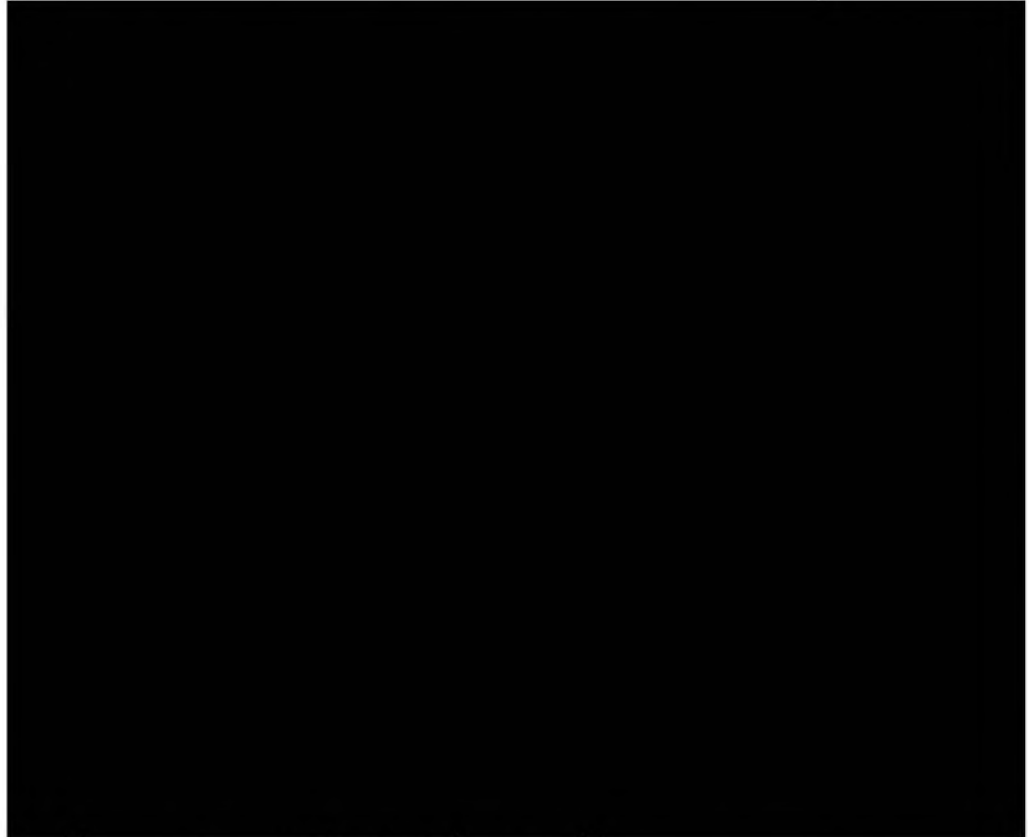
1. subject may have been convicted of a criminal offence.
2. a warrant is outstanding.
3. subject may have criminal associates.
4. you deem it advisable to clarify information or assess sources.
5. otherwise specifically directed.
7. If you wish to conduct credit bureau check, follow procedure in F. 7. f. 1.

2. Inquiries and Interviews.

1. When it is necessary to take a PHF on an investigation.
 1. follow proper security procedures.
 2. take precautions to protect contents from accidental disclosure.

3. do not show PHF to sources.

2. When making inquiries, the following sources of information should be considered:



3. To the fullest extent possible, interview only respected responsible members of the community who have personal knowledge of the subject of inquiry.
4. Fully explain the reason for the inquiry and the importance to the security of Canada of obtaining an informed, truthful appreciation of whether the subject

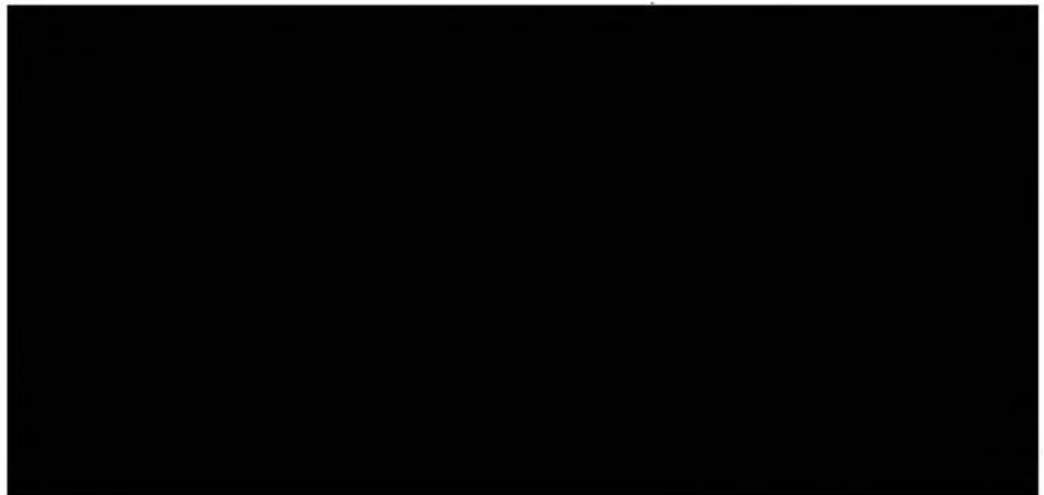
8. In the event your enquiries, or interviews, lead you to believe that a complaint may be lodged, or that criticism will be forthcoming in the public forum, immediately provide Headquarters with a report outlining all the circumstances.

*Addition
Page 34*

is one in whom the government may repose full trust and confidence.

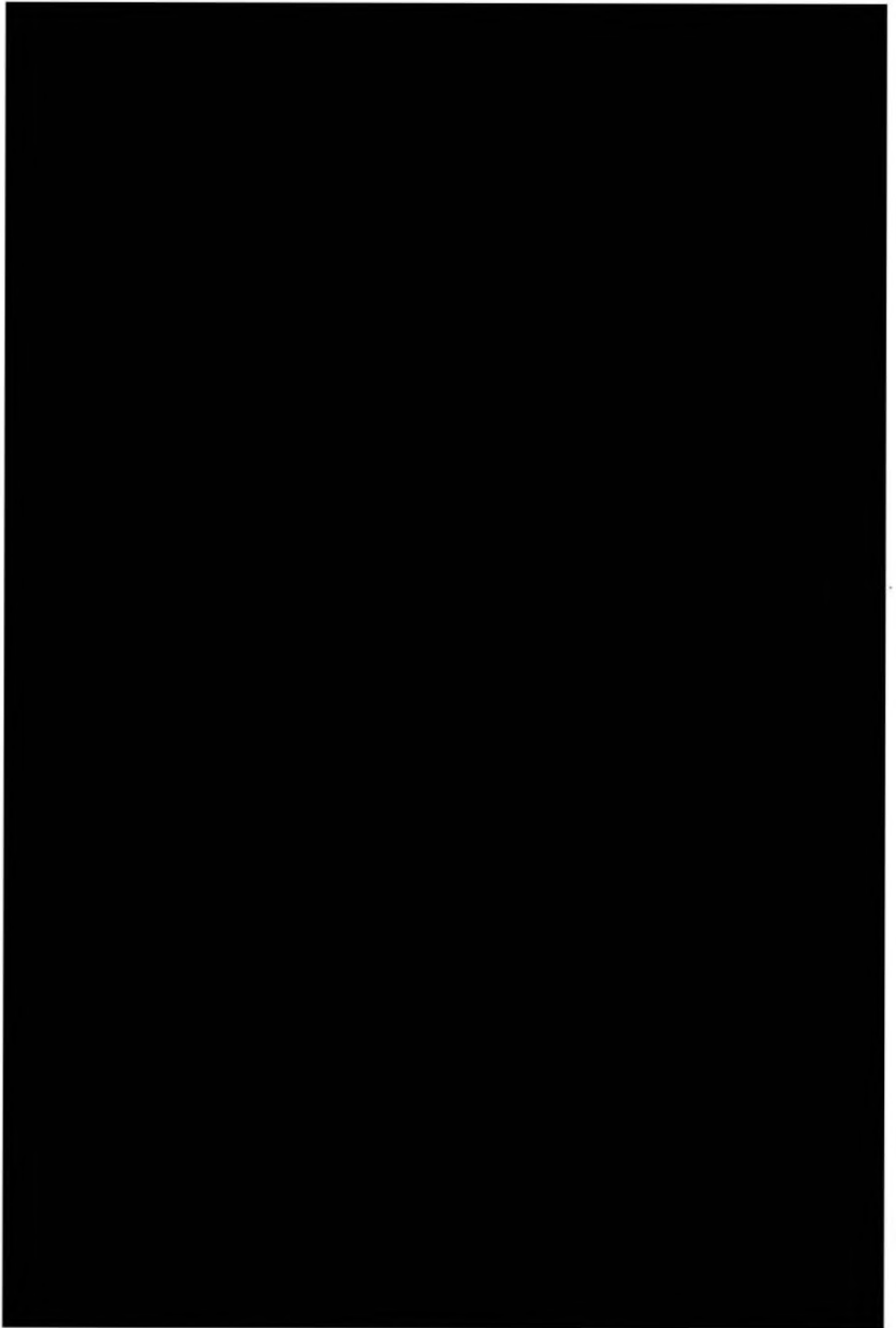
5. If a source is hesitant about providing information, fully explain the protection for sources found in sections 22 and 23 of the Privacy Act.
6. Keep questions brief, uncomplicated and unthreatening and, attempt to put person being interviewed at ease.
7. Do not disclose information that has been provided by other sources.
8. While circumstances will dictate the approach to be taken during the investigation, ensure that all inquiries and interviews relating to traits of character, lifestyle or personal circumstances, e.g. homosexuality, venality, alcoholism, debt, gambling, are conducted with sensitivity, tact, discretion, maturity of judgement and absence of bias.
9. Where source is in a position to appreciate the importance of access to classified information, seek the sources opinion as to whether the subject should be granted a clearance supported by his/her reasons.

10. Where adverse information surfaces during the course of an inquiry, attempt to the fullest extent possible to obtain independent corroborative information.
11. Explore fully how the subject copes with alternate lifestyle, e.g. homosexuality, with emphasis upon 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 record access to which may be prohibited by law or a professional code of ethics without a specific consent form from the individual to whom the record relates.
13. When making inquiries or conducting an interview, explore the following areas:



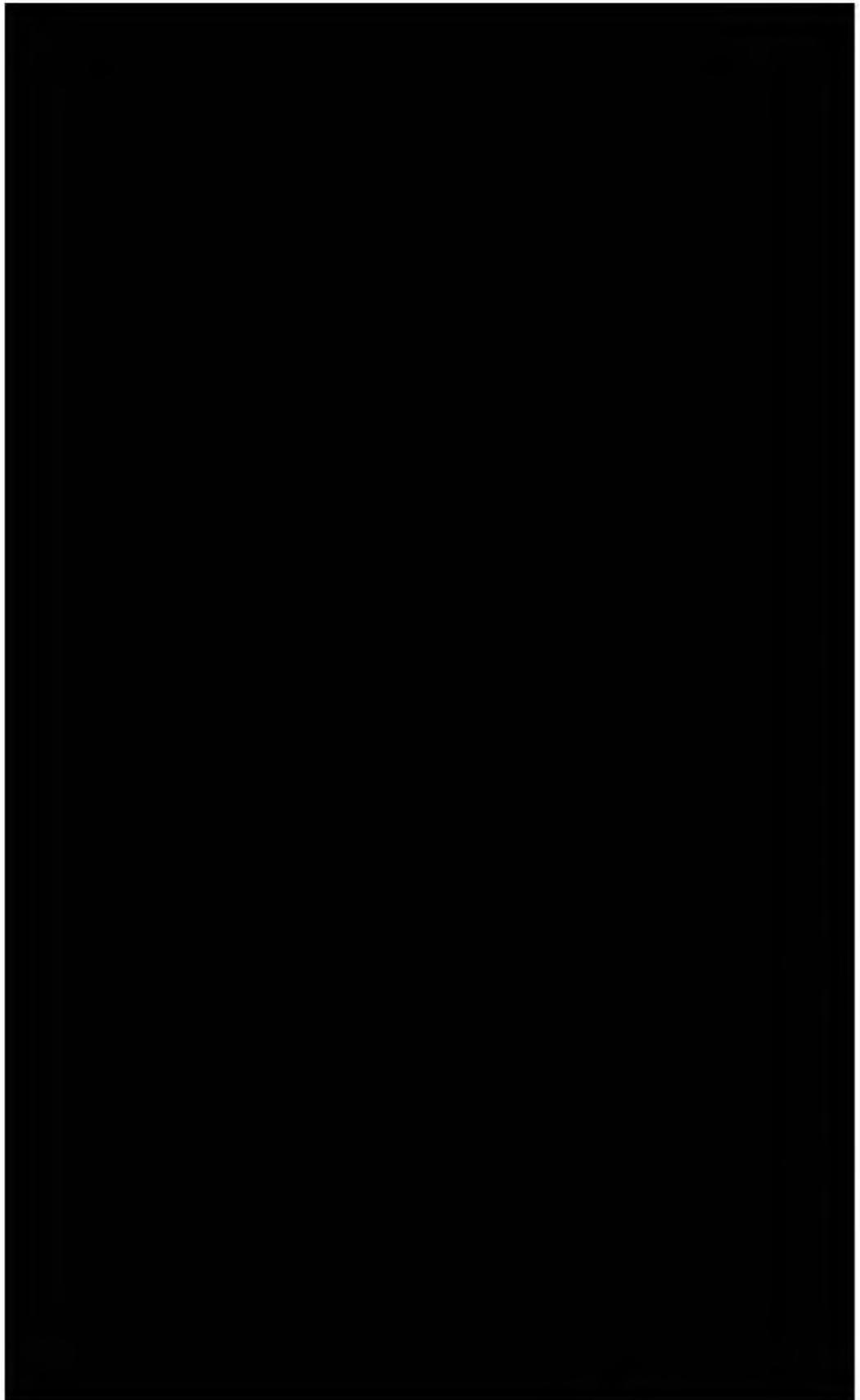
s.15(1)

s.16(1)



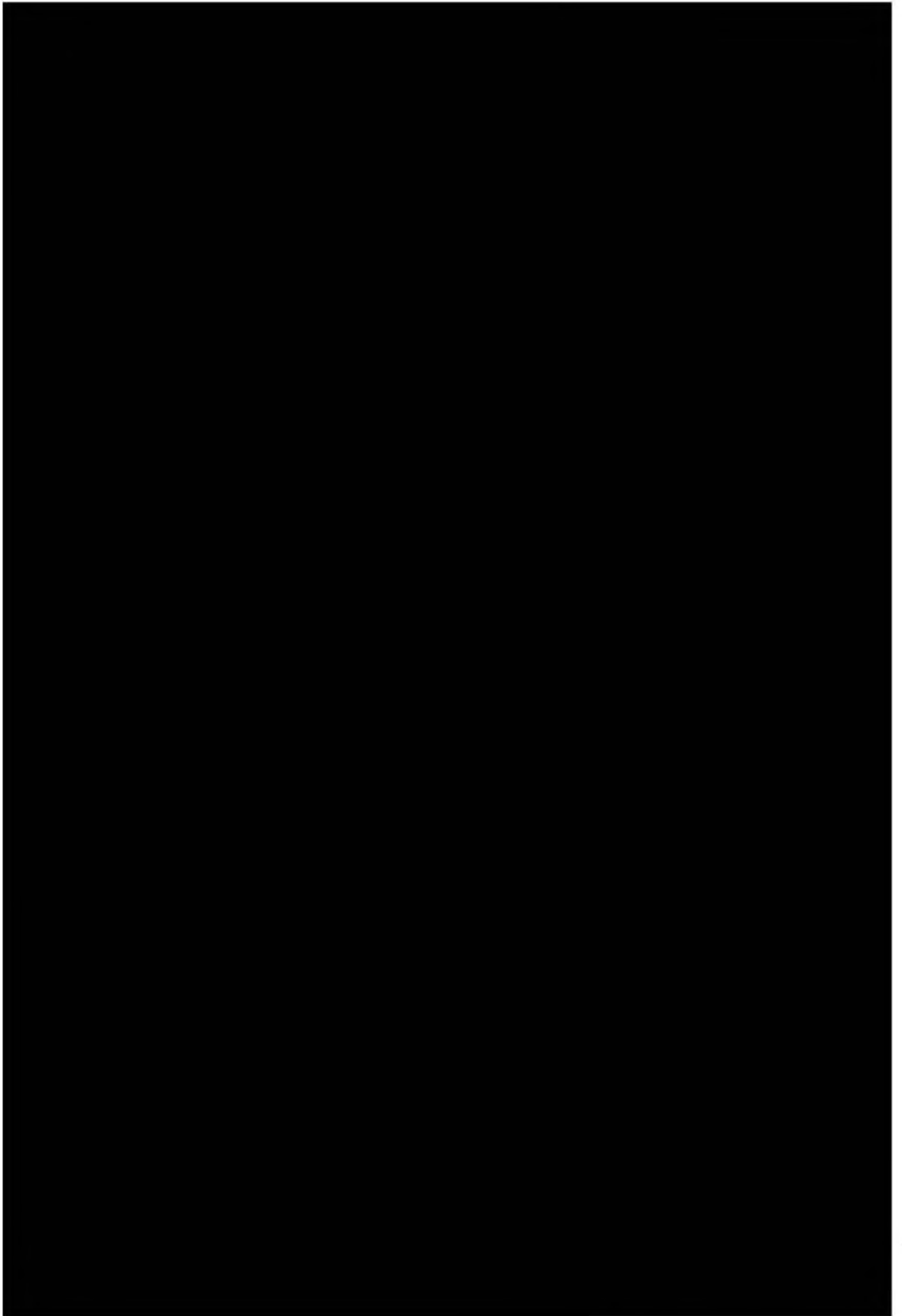
s.15(1)

s.16(1)



s.15(1)

s.16(1)





14. When information surfaces from a source that the subject of inquiry may support separatism, do not explore with source beyond that which is necessary to satisfy yourself as to the basis for source's belief.
15. When adverse information surfaces during an investigation, ask HQ to authorize an interview of the

subject. The purpose of the interview is to:

1. provide the individual an opportunity to explain his actions or refute allegations.

2. provide the investigator the opportunity to [REDACTED]

[REDACTED] come to his own informed opinion as to whether subject ought to be given a security clearance.

16. To ensure the protection to sources offered by Sec. 22(1)(b)(ii), P.A., when a DSO requests an investigation on the basis of suspicion that grounds may exist to remove or downgrade a security clearance, establish from each source contacted if the cooperation being extended is in confidence and clearly indicate this in your report.

F. 10. g. 3. Reporting

1. Report all information developed that is relevant to the determination of whether subject ought to be given a security clearance.

2. Report only security relevant information except where

investigation is in respect to an employee of the Security Service in which case submit a separate report on any information positive or negative developed which may speak to subject's suitability for employment.

3. When circumstances are believed to exist about an individual, which cannot be determined as factual, and the investigator is satisfied that the information is true although it could not be corroborated or confirmed, clearly indicate that information is believed to be true but has not been substantiated.
4. When the comments of a source are such that you do not know whether to believe them or not, clearly indicate that information is unverified and is being reported without any assessment of whether it is likely to be true.
5. Avoid any subjective comment as to whether the subject should be afforded access to classified material.
6. Provide comment where you have formed a valid opinion during the investigation or interview that a subject's character, beliefs, or lifestyle could have a bearing on his or her loyalty.

7. Provide a full assessment of all sources reporting, including:

1. their relationship to the subject of inquiry, i.e. social, working, recreational, casual.
2. apparent knowledge of subject over what period of time.
3. any indication of dishonesty or bias for or against subject.
4. basis for any belief or opinion expressed.
5. expectation of confidentiality in accordance with F. 10. g. 2. 16.

8. RCMP Detachment

1. When sending information through channels use form C-237 and submit it in the format shown in App. II-8-5. See Admin. Man. XI.4.
2. If several sources provide identical assessments, combine the remarks in one paragraph, otherwise

report the information in separate paragraphs.

9. Area Command

1. Use secure communications facilities to transmit security screening reports to Headquarters.

1. If you do not have access to secure facilities, use Form C-237. (See Admin. Man. XI.4.)

F. 11. Preparation of Intelligence Assessment

F. 11. a. Policy

1. Information having a bearing upon whether a person ought to be granted or retain a security clearance shall be reported by "HQ" "A" Operations to the responsible government institution in the form of a factual report in which all sources have been fully assessed in terms of their reliability.
2. Assessments shall not contain a recommendation for or against a security clearance.
3. Any relevant open information that can be safely

disclosed shall be included with the assessment to the ISO.

4. Except where there are reasonable grounds to believe the subject of security screening procedures is under the undue influence of a close relative or associate, aspects relating to reliability, i.e. greed, debt, homosexuality, criminal record, or evidence of support for separatism in respect to the relative or associate is not relevant to the security status of the subject and shall not be reported or otherwise commented upon in an intelligence assessment.

11. b. General

1. An individual subject of security screening procedures may make application under the Privacy Act to see the intelligence assessment provided to the government institutions together with any report or document relating thereto. 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. This means that if a member engaged in security screening duties reports only to those to whom he has a duty to report and confines himself to accurate statements of what he has

been told and any verification or lack of it, he will not incur liability for slander or libel. Reporting as true a fact which one knows to be untrue could constitute malice.

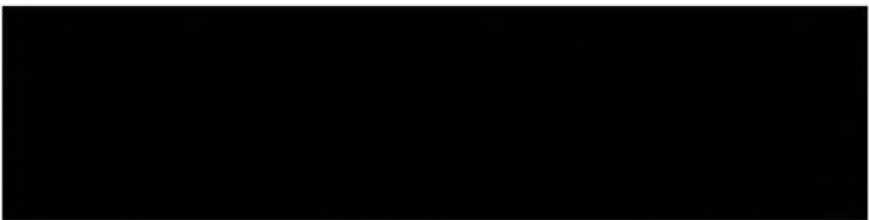
U. 11. c. "A" Cps - [REDACTED] Unit

1. Prepare an intelligence assessment to the DSO including only those allegations or facts which are fully and factually reported and where identification is based on information provided by sources whose reliability has been properly assessed.

2. Loyalty

1. describe the activities of the subject in terms of their relevance to para. 3 and 4 of C.D. 35.
2. where the subject has at one time been a member or supporter of an organization described in para. 3 of C.D. 35, describe to the extent known, his or her reasons for discontinuing membership or support.
3. where the subject has family or other close continuing relationship with persons described in paras. 3 and 4 of C.D. 35, describe, to the extent

known, the degree of and circumstances surrounding, such relationship and most particularly the degree of influence that might be exerted on the subject to act in a manner prejudicial to the security of Canada.

4. where the subject 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 subject to act in a manner prejudicial to the security of Canada.
5. to the extent possible report only activities that have been corroborated by independent sources.
6. 
7. ensure sources, methods of operation and targets of the Security Service are adequately protected in the intelligence assessment.
8. provide a full assessment of the risk to security posed by the subject in terms of paras. 3, 4 and 6(b)(c) of C.D. 35, but avoid any recommendation as to whether he/she ought to be granted a security

clearance.

9. when including information that a person may support separatism ensure that the information is fully qualified in terms of its reliability and its currency.
10. in all cases where information reported is uncorroborated or otherwise uncertain, clearly note this in the assessment.
3. Reliability as it relates to loyalty.
 1. Provide a full explanation and assessment of the vulnerability of subject to indiscretion, dishonesty, compromise or blackmail based upon his/her activities or features of character as described in para. 6(a) of C.D. 35.
 2. In all cases where information of a type described in para. 6(a) of C.D. 35 is uncorroborated or otherwise uncertain, clearly note this in the assessment.
 3. Ensure sources, methods of operation and targets of the Security Service are adequately protected in the intelligence assessment.

4. Avoid any recommendation as to whether the subject ought to be granted a security clearance.
4. Attach to the assessment an approved profile of the organization(s) to which subject or his close relatives or associates have belonged when the organization:
 1. has been assigned a level of investigation by OPRC.
 2. is now defunct or altered in character but was, at the time of subject's contact or involvement, an organization which had or would have had OPRC approval.
5. Nothing in F. 11. c. 4. precludes comment upon subject's involvement in other legitimate organizations in the body of the assessment providing such involvement is in some way relevant to subject's security status and it is made clear the organization itself is not in any way considered to be subversive in character.
6. When adverse information has surfaced from a sensitive source or in a current operational context, on a person holding a security clearance:

1. Consult with the appropriate [REDACTED] branch to determine the appropriate level at which the information can be disseminated.
2. Forward to the department any information that can be disseminated and place SSF 213 inside front cover of operational category file.
7. When subject of PHF is an employee of, or candidate for employment with the Security Service, provide a separate report of any information developed which relates to suitability for employment in other than a security sense to Officer i/c Staffing and Personnel.
8. Ensure that organizational profiles are updated by the appropriate [REDACTED] branch on a regular basis.
9. Branch Commanders
 1. Provide assessments and advice in cases involving your operational responsibilities upon request.
 2. Provide or update organizational profiles upon request.