9411114

TABLE OF CONTENTS

F. Field Tasking and Investigations

F.1. General
F.2. Headquarters Analysts
F.3. Investigator
F.4. Individuals in Sensitive Institutions
F.5. Processing CSIS Act Section 19(2)(a), (b), (c) and (d) Information

G. Security Assessment

G.1. [redacted]
G.2. Analyst
G.3. Allegations of Security Concern
G.4. Security Assessment of Juveniles
G.5. Upgrades/Downgrades
G.6. Quality Control
G.7. Incomplete Assessments

H. Special Requests

H.1. Airport Restricted Area Access Clearance Program (ARAACP)
H.2. Ministry of Foreign Affairs and International Trade
H.3. Department of National Defence (DND)
H.4. Royal Canadian Mounted Police (RCMP)
H.5. Canadian Security Intelligence Service (CSIS)
H.6. Order-in-Council Appointments
H.7. Ministerial Staff
H.8. Departmental Security Officers (DSO)
H.9. Foreign Security Screening
H.10. Security Breaches

SECTIONS I. AND J. CAN BE FOUND ON FILE "SSPM IMM ENGLISH"

I. Citizenship Applications Procedures

I.1. References
I.2. Issues
I.3. Responsibilities and Procedures - Citizenship Rejections
I.4. Identifying Potential Threats - [redacted] List
I.5. Deportation Proceedings
I.6. Regional Responsibilities - Citizenship Interviews

J. Immigration Screening Procedures

J.1. References
J.2. Issues
J.3. Responsibilities and Procedures
J.4. Preliminary and in-depth security interviews at posts overseas and in Canada and the USA

A. LOYALTY, AND AS IT RELATES THERETO, RELIABILITY

Within the Security Screening program the terms loyalty, and as it relates, reliability, have specific meaning. Three key documents provide explanation and definition of these terms: the CSIS Act, the Ministerial Directive, and the Government Security Policy (GSP).

The CSIS Act stipulates the Service may provide security assessments, defined as:

> "an appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual (S.2 CSIS Act)."

Loyalty is defined in terms of four activities based upon threats to the security of Canada. Reliability is a concern if it can be related to loyalty. Thus, a clear causal relationship between loyalty and reliability must be seen to exist between the two before it warrants Service attention. Derogatory information about the subject's character or personal habits has relevance only from the perspective of coercion, compromise or blackmail, ie. as it may affect loyalty. Likewise, with the emphasis on assessment as an appraisal of loyalty to Canada, the Service is not concerned about an individual's political beliefs or associations, but rather whether the individual engages in activities that represent a threat to the security of Canada.

One may wish to examine an individual against a continuum. At one end is loyalty, where activities and threats to Canada are addressed, and at the other end is personal suitability, where qualifications and work habits are dealt with. In between and related to both loyalty and suitability is reliability.

Personal Suitability — Reliability — Loyalty

Whereas threats to the security of Canada are outlined in Section 2 of the CSIS Act, the GSP and the Ministerial Directive on the provision of security assessments establish the "evidentiary standards, tests, and rejection criteria" (Appendix F of the GSP) by which a person can be denied a security clearance. These documents reinforce the fact the Service provides informational facts, and an assessment of the individual's loyalty to Canada and a recommendation to the requesting department advising whether the clearance should be granted or not. If the concern is a reliability factor the causal relationship to loyalty must be clearly identified. The Ministerial Directive stresses a screening investigation must balance the need to provide an assessment with the rights of the individual. There is a limit to the scope of the inquiries related to the degree of threat.

The definition of loyalty flows from Section 12 of the CSIS Act:

Espionage/sabotage, foreign interference, political violence and undermining democratic institutions. However, these are still rather broad categories, and the HQ analyst should have examples which highlight such concerns. There are numerous screening requests which do pose concerns which raise questions about the subject's loyalty. These must be resolved through screening investigation, analysis and assessment. There are three types of concerns encompassing [redacted] questions:

1) Trace information which indicates the subject may engage, or be engaged in espionage, foreign interference or political violence, such as:

[redacted]

2) Factors of circumstance concerning the subject which raise questions about commitment and loyalty to Canada, such as:

[redacted]

3) Association with groups or individuals who may call into question the legitimacy of Canada's democratic institutions (s.2.d). In these cases, the concern is predicated upon whether the subject is or was:

[redacted]

One may also define three major concerns associated with reliability, as it relates to loyalty:

1) Whether the subject is trustworthy and respects the confidences of others.

2) Whether the subject has certain character traits or behaviour problems that may affect loyalty due to the possibility of compromise, coercion or blackmail (ie. substance abuse, sexual misconduct, criminal or financial problems).

3) Whether information raises doubts about the subject's honesty and judgement. Loyalty would be called into question if an individual was in contact with persons of interest pursuant to Section 12, and displayed disregard for security precautions.

4) Incomplete documentation from the subject, which may be an oversight, or a question of dishonesty and falsification.

The definition of loyalty and reliability as it relates thereto is predicated first and foremost upon the CSIS Act in its identification of certain threat activities. The GSP and Ministerial Directive provide the standards and test criteria used in making our security assessment and recommendation. These suggest in turn certain basic questions about the subject's loyalty and reliability which will trigger investigative action and indicate points of departure for the HQ analyst. A full listing of the concerns and how the human condition and reactions to them may be interpreted is found in Guide to Investigators. Certain terms and procedures are also described in more detail in the appropriate sections of these Procedural Guidebook.

B. PROCESS AND DECISIONS - GENERAL - GOVERNMENT SCREENING

B.1. Initial Processing Steps

Security assessment requests from government departments and allied agencies are directed to the [redacted] Section. [redacted] personnel are responsible for opening the appropriate security screening file where applicable, and conducting an initial quality control check of the GSP documentation received. The Unit forwards the subject's fingerprints to the RCMP, if applicable, or conducts a CPIC check, for processing and conducts CSIS indices check, and credit bureau check if applicable. Depending on the result of the CSIS indices check, [redacted] may be sent to the [redacted] where a decision is rendered as to whether the subject [redacted] For those requests where [redacted] has not been delegated the responsibility to provide Notices of Assessment, the results of these checks and all relevant material are sent to the Security Screening Analysts for further processing and security assessment evaluation.

B.1.2. Security Screening files and Security Screening Request Numbers (SSRN) received by the [redacted] Unit, and sorted according to the portfolio unit designation.

B.2. Secondary Processing Steps

The following steps, (outlined in a chart (Att. B.2.1) in the paper version) outline the process to be followed and the decisions to be made in the conduct of a security clearance investigation and the transmittal of a recommendation to a 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 recommendation to grant for Level 1 and 2 requests, or proceed further because of traces, or because a Level 3 field investigation is required.

B.4. Evaluation of Initial Indices Checks

The analyst evaluates all available information which could or might affect an individual's security clearance status ([redacted]). The analyst decides, based on the nature of the information, whether to assess the information as not being of security concern, and prepare a standard security assessment or 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. It may also be necessary to request an assessment [redacted] identifying any security concerns presented. 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 prepares a request for the appropriate out-of-country check(s).

B.6. Decision on Tasking

The analyst decides on the tasking to be requested of the field or allied service. The information available will suggest certain questions to 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 subject is being considered for a Level 3 security clearance, the analyst will task Security Screening field offices in all Regions where the subject has resided [redacted].

B.7. Evaluation of Field Reports

There are five general criteria by which 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 subject 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 assesses all the information gathered and decides on its relevance and sufficiency. Where there is no adverse information, a favourable reply may be sent to the requesting government institution. However, there may be trace information or "features of character" such as substance abuse, financial problems, criminal behaviour, etc. If the analyst determines that the investigation is deficient in coverage, the analyst must address this concern by re-tasking the field through the Unit Head. 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 the investigation is as complete as possible and has resolved all concerns, the analyst then makes a judgement on what is, or is not significant, recommends the appropriate action, and prepares an assessment.

B.9. Summation and Initial Conclusion

The analyst prepares a short summary of the relevant security information and background of the case, and recommends whether the subject should be granted or denied a security clearance. In the case of an information brief or a denial, the recommendation and all relevant documentation are forwarded to [redacted]

B.10. Review and Evaluation

The [redacted] analyst reviews the complete file and makes a similar evaluation. If the [redacted] analyst is not satisfied with some aspect of the investigation these concerns are outlined to the Sector Manager and Unit Head who may then re-task the field to address the concern, thereby permitting further enquiries for the collection of additional information considered essential.

B.11. Decision on Reporting

When satisfied that the investigation is complete, the [redacted] analyst assesses the available information to determine what should be reported to the requesting government institution in order that a 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 identifying what was done; comments on the loyalty and reliability of the subject, and makes a recommendation regarding the granting of a clearance to the subject. The assessment is based on all available information, favourable or unfavourable, and must not reflect the [redacted] analyst's personal preferences. (See Chapter G for greater clarity)

B.13. Review and Recommendation

[redacted] reviews each assessment to ensure consistency in quality and in support documentation. The final recommendation to the requesting department is made in accordance with the signing authorities chart. (See Attachment L.4) If a recommendation for denial is considered, the agreement of DG Security Screening, Deputy Director Operations, Legal Services and the Director is required.

B.14. Sign-off to Requesting Department

The final detailed security assessment is then signed off to the requesting government institution.

*Note: Attachment B.2.1. is located in the Procedures appendices.

C. [redacted] SECTION [redacted]

C.1. General

All GSP documentation, including the Personnel Security Clearance Questionnaire (PSCQ) are received by [redacted] to be clocked in, counted, prioritized and pre-screened.

The PSCQ are then given to the [redacted] who proceed to verify all names [redacted]. In accordance with item E.2.1.a., where possible files exist, the information is sent to the Security [redacted] Section for identification and returned to the [redacted] for creation of an SSRN. Where required, subject's fingerprints are sent to the RCMP, and a credit bureau check is completed. All relevant information is recorded [redacted]. (Exception: those requests from RCMP are checked against CSIS indices only, and stampbacked. In cases of a "HIT", or request for an out-of-country check, a file may be opened if requested and then sent to the Security Screening Branch.)

- Use the CSIS [redacted] "clocked in date" as the Date of Request, in order to compute the CSIS turnaround time for processing the clearance.

C.2. Review

Security assessment requests will be processed as follows:

C.2.1. [redacted] will load the basic data [redacted] for all government security screening requests.

C.2.2. The only time [redacted] will automatically load the full data [redacted] and [redacted] is for Government level 3 requests.

C.2.3. Full data and [redacted]) file for all other cases will be done on request from the analyst only.

C.2.4. When [redacted] has completed their task, they will forward the screening requests which require further review by the analysts to [redacted].

(a) Security assessment requests where "Basic Reliability" or "Enhanced Reliability" status has been granted.

Documentation Required:

- Security Clearance Requests and Authorization Form (TBS 330-23).
- Consent Form (TBS 330-58).
- Reliability Check Report (TBS 330-71)
- Personnel Security Clearance Questionnaire Form (TBS 330-60).
  (N.B. A record of decision concerning any reliability issues that have been decided in favor of the individual and that justify proceeding with a security clearance request.)
- For Level 1/2: results of the Criminal Records Name Check. If the CRNC surfaces a record, the departments will have conducted a fingerprint check and, in this case, the documentation must include the results of that check.
- For Levels 3, the documentation must include the Fingerprint Form except for update, when a CPIC check is permitted (RCMP C-216C). [redacted] staff should process this form in the normal fashion by requesting a RCMP fingerprint check, where this has not been done by department. The department must also provide a credit check.

[redacted] Action Required:

- conduct quality control inspection of documentation received;
- arrange for fingerprint or CPIC check, if necessary;
- conduct credit bureau check, if necessary;
- conduct CSIS indices check;
- open file if required;
- [redacted]
- sort according to priority and then determine whether request involves a clearance "update" or is made in respect of "new start" (i.e. the employee does not have a current, valid security clearance);
- process "new start" before "update" requests; and
- conduct further processing as detailed in C.3.

(b) Security assessment requests without either a "Basic Reliability" or "Enhanced Reliability" notification.

These requests will fall within one of the following categories:

- PWC
- SSC
- CSIS

- Foreign Requests
- Airport Access

Documentation Required: (except for Foreign)

- Basic Reliability Documentation.

[redacted] Action Required:

- Requests received for CSIS require arrangements for fingerprint and credit bureau checks. Quality control is required for those received under the Airport Access Program, PWC or SSC; and CSIS applicants.
- sort and process requests as per Basic Reliability.
- conduct further processing as detailed in C.3.

C.3. Processing - Levels 1/2

C.3.1. [redacted] has been delegated the responsibility for providing Notices of Assessment for levels I and II priority "D" and "E" requests, and for supplementals for levels I and II, where there is no trace information.

Attachment C.3. outlines those activities which are necessary in the review and processing of requests described earlier.

"No Trace" information stems from verifications of:

1) [redacted]
2)
3) RCMP Indices Check (fingerprint and/or CPIC/CRNC)
4) Credit Bureau
5) PSCQ check: [redacted]

C.4. Processing - Foreign Checks

REFERENCE: IP 371-1 - Memo from [redacted] dated 91-05-16

C.4.1. In addition to the usual procedures, [redacted] will process foreign checks ([redacted] Files) as follows:

a) [redacted]

b) Classification sheet:

This sheet will only reflect the following information:

i) subject's name, DPOB and address,
ii) spouse/co-habitant only, with DOB,
iii) country code,
iv) [redacted]

c) Indices checks:

i) CPIC checks [redacted]

ii) CSIS checks on [redacted]

C.5. Processing - CSIS Applicants

REFERENCE: Memo DG SIS to DDG Records [redacted] / 1992.07.21

C.5.1. Conduct a CPIC Check [redacted]

*Note: Appendix C.3. is located in the Procedures appendices.

D. FORMS AND FILES

D.1. Personnel Security Clearance Questionnaire

REFERENCE: 1. Operational Manual II.4 Appendix G
2. Memo from DDG Records, 89-04-18, IP371-1

Screening Analyst:

D.1.1. Personal information necessary for security screening enquiries is provided by the subject and forwarded to the Service by the requesting department on a Personnel Security Clearance Questionnaire (PSCQ).

[redacted]

[redacted]

D.2. Diary Date

REFERENCE: 1. OSS Annual Plan
2. Letter from PCO to Director dated 5 Feb 87

D.2.1. Headquarters Security Screening

(a) Refer to Attachment D.2.1.a. to determine the priority of the request and the corresponding diary date.
(b) When tasking the field, indicate the priority and the subsequent diary date.
(c) If the diary date has not been complied with, request a report from the regional office.

D.2.2. Field Investigators

If the diary date cannot be complied with, request an extension and provide the reason.

D.3. Restricted File Holdings

REFERENCE: 1. Letter from A/DDG Records/Infoman 20 Oct 89 pursuant to SIMRMRS/1186/49 dated 30 June 89 on file [redacted]
2. Telex [redacted] dated 89-11-21, file IA565-138-5, regarding [redacted] access to restricted file holdings.

D.3.1. [redacted]

D.3.2.

[redacted]

D.3.3.

D.3.4.

D.3.5.

D.4. Cancellations

Cancellation letters received from the Government Departments for [redacted] cases must be cancelled through [redacted]

Once the cancellation has been completed, the letter should be destroyed.

D.4.1. Administrative Cancellation by Department

(a) [redacted]:

1. Receive cancellation notice of a security clearance and place on subject's [redacted] file, and enter in [redacted] destroy the notice.

D.4.2. "In Process" Cancellation by Department

(a) [redacted]

1. Receive notification of cancellation of clearance request, and place correspondence on subject's [redacted] file.
2. Forward file to appropriate Security Screening Branch portfolio unit.

(b) Analyst:

1. If a field enquiry has been initiated immediately notify the field by telephone to cancel the request, followed by confirming message.
2. Record cancellation in [redacted].
3. Return [redacted] files to Records.
[redacted]: Also logs in manual log)

D.4.3. "In Process" Cancelled by Field

(a) Analyst:

When you receive field report indicating subject no longer requires security clearance:
1. Check [redacted].
2. Telephone Department for verification of cancellation, and request written confirmation.
3. Notify other regions involved via phone and/or message to cancel further investigations.
4. Record cancellation in [redacted].
5. Return file to Records.
6. When cancellation notice is received, enter in SSIS.

D.5. [redacted]

REFERENCE: 1. Signing Authorities Chart
2. Memo from DDG dated 89-10-20, file IP371-1

D.5.1. When guidelines permit, a [redacted] may be used to provide recommendation to the requesting agency.

D.5.2. [redacted] will generate a form which reflects the data entered. Ensure the proper completion of form with particular attention paid to the following:

1. Classification - PROTECTED
2. Date of request - date the request was

forwarded to CSIS by the DSO.

3. Level Requested.
4. Recommendation

[redacted]

D.5.3. If security-related information exists which may impact on the decision rendered by the DSO, [redacted]. Provide all relevant information to [redacted] for a detailed security assessment.

D.5.4. For requests from [redacted] CSIS, any trace of potentially negative information must be briefed to those departments.

D.6. Caveats

REFERENCE: 1. Operational Manual Bulletin #OM 37 - 91/01/23 (IV.1) (Appendix D.7.)

D.6.1. In addition to those caveats described in Appendix D.7., the following caveats are also used within Security Screening:

(a) [redacted]

(b)

[redacted]

(c) [redacted]

D.7. Opening [redacted] Files with [redacted]

D.7.1. How to have an [redacted] File Opened

Analyst:

Complete the B-17 Request Form and attach to the screening package.

Before you send the request to B-17 record this activity [redacted]

Once [redacted] has been created, [redacted] will forward the file [redacted] following the same procedures which applied previously.

D.7.2. Out of Country Checks

If out of country checks are necessary and there is no evidence at this time that further enquiries are necessary, [redacted]. If further enquiries are to be conducted regardless of the

results of the foreign checks, [redacted]

To initiate an out of country check:

(a) [redacted]

(b)

(c)

(d)

[redacted]

Please note that the steps in sending out of country checks remains the same. The proper documentation must be sent along with the letter to the SLO or IPM. [redacted]

[redacted]

[redacted]

D.7.3. Consultation with [redacted]

Analyst:

[redacted]

D.7.4. GSP Level 1 & 2 for Cause

[redacted]

D.7.5 Field Taskings

[redacted] are required for all field taskings to the regions, or for an out of country field.

Analyst:

[redacted]

[redacted]

D.7.6. Bring Forward (BF System)

Analyst:

[redacted]

D.7.7. Correspondence with H.Q. [redacted]

Analyst:

[redacted]

[redacted]

D.7.8. Formbacks - Sending Another Copy

Analyst:

When a screening case has been concluded and the dept. has been given a NRT Decision but does not receive the original formback send the dept. another one.

[redacted]

D.7.9. Amending PSCQ Requests

Analyst:

Any changes required to a subject's D.O.B., surname or given name must be sent to the attention of an [redacted] supervisor in order for all the proper checks to be re-done. [redacted]

ATTACHMENT D.1.1.h.

LIST OF COUNTRIES OF SECURITY CONCERN

[redacted]

* Designated Countries

ATTACHMENT D.2.1.a.

PRIORITIES AND DIARY DATES

Priority A	-	Order-in-Council Appointees
	-	Judicial Appointees
Priority B	-	Ministerial Exempt Staff
Priority C1	-	CSIS
Priority C2	-	Airport Security
	-	Communications Security Establishment
	-	Departmental Security Officer Positions
	-	DSS Special Defence Projects
	-	Foreign Service Officers of Ministry of Foreign Affairs and International Trade/Health and Welfare
	-	Inspector General and SIRC
	-	NATO Clearances
	-	RCMP Regular Member engagements for Depot
	-	Special Cases - as confirmed by the DG-OSS
Priority D	-	All other Institutions
Priority E	-	Updates to clearances

Note: Appendix D.7. is located in the Procedures appendices.

E. INDICES VERIFICATION

E.1. Documentation Required

E.1.1. Basic and enhanced reliability checks are not security clearances. A basic reliability check is a condition of appointment to the Public Service and is conducted by government institutions for all appointments, assignments (including secondment and interchange) and contracts for service of less than six months duration. An enhanced reliability check is conducted by government institutions when an appointment, assignment or contract involves the care and custody of, or access to, sensitive information or sensitive or valuable assets that are not classified in the national interest.

E.1.2. Security clearance investigations may be conducted and information disclosed to government institutions in response to requests for clearances in the following categories:

(a) Level 1/2 requires:

- a basic or enhanced reliability check conducted by requesting department;
- either a fingerprint check or a name check for criminal records;
  (NOTE: If record found, fingerprints are required to confirm identity)
- CSIS indices checks;
- a check of Credit Bureau records (optional);
- a check of foreign agency indices, if applicable;
- a field investigation and/or subject interview "FOR CAUSE"

NOTE: For Level 1 and 2 the investigation should normally cover a 10 year period or to the subject's 16th birthday.

(b) Level 3 (Top Secret) requires:

- in addition to the checks required for Level 1/2
- a check of foreign agency indices, if applicable, including field enquiries;
- a field investigation normally covering the preceding 10 year period or to the subject's 16th birthday; and
- a subject interview, if deemed necessary;
- mandatory credit check;
- fingerprint check, or CRNC on updates.

(c) Site Access Security Clearance
(SPIN 1991-02, TB, dated 25 JAN 1991)

Site access security clearances will be limited to two types of programs.

1. those involving work sites or facilities which are designated, on the recommendation of the Director, as ones which could reasonably be expected to be targeted by those who engage in activities constituting threats to the security of Canada as defined in the CSIS Act. Contracting authorities are required to submit such proposals to Treasury Board for its recommendations; or
2. for those authorized by statute or regulation (e.g. Aerodrome Security Regulations).

3. Such clearances are to be transferable from one site access program to another, but are not to be taken as equivalent of level 1 clearances.

E.1.3. The requirement for security clearance updates is five years for Level 3 clearance and 10 years for Level 1 and 2 clearances. Updates may also be performed at any time 'for cause' or at the discretion of the Deputy Head.

E.1.4. 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 subject is being considered for and the classification of assets to be accessed.

E.2. Security Screening [redacted] Unit
(Memo from DG Security Screening to Records; IP 371-1 dated 91-02-06)

E.2.1. Check PSCQ against CSIS indices

(a) [redacted]

[redacted]

(b) [redacted] Analyst

Check PSCQ against CSIS indices (trace information)

1. Files may be analyzed as:

- [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

7.

8.

9. Forward all PSCQs and attachments to [redacted]

E.3. [redacted]

REFERENCE: 1. [redacted] dated 89-11-21 on file IA565-138-5.
2. Memo dated 26 June 1987 on file IP371-1, re: [redacted] Printouts.
3. Memo dated 29 January 1990 on file IP371-1; re: [redacted] Checks

E.3.1. Access information or conduct queries of [redacted] for all background checks, ensuring identity of file subject is the same as the results of the [redacted] search.

E.3.2. Conduct [redacted] checks:

(a) [redacted]

(b)

(c)

(d)

(e) [redacted]

(f)

(g)

(h)

(i)

E.3.3. [redacted] checks will be conducted by HQ staff prior to any investigation sent to the field.

E.4. CSIS Act - [redacted]

REFERENCE:
1. Memorandum dated 88-06-06, Airport Security Program, file IP371-1
2. MD - Provision of security assessments
3. Bulletin CSIS OM 21 - Reporting of Unsolicited Information
4. IP371-1 memo to DDG Records re: SS Coordinators
5. Memo 15 NOV 90 [redacted] from DDG Records
6. Memo 20 MARCH 87, IP371-1 Head, Services [redacted]

E.4.1. Restriction of Access to Security Screening Files

(a) All information collected, retained or reported by the Service pursuant to section 13, which the Service is precluded from collecting, retaining or reporting [redacted]

1. [redacted]

2.

3.

4. [redacted]

E.4.2. [redacted] Traces

(a) [redacted]

E.4.3. [redacted] Consultation

Analyst:

(a) [redacted]

E.4.4. Use of [redacted] Information

(a) [redacted]

[redacted]

E.4.5. [redacted] Information obtained during the course of a Section 15 investigation

(a) [redacted]

(b)

E.5. [redacted]

REFERENCE:
1. Memorandum dated 20 October 1989, Government Screening, Chiefs and Heads Meeting, file IP317-1.
2. Memorandum dated 3 November 1989, Security Screening Investigations [redacted] file [redacted]
3. Memorandum dated 1 May 1989, Interim Measures for [redacted], file IP371-1.
4. Operational Manual, II.6.E.4.

E.5.1. [redacted]

(c) [redacted]

(d) [redacted]

(e) [redacted]

E.6. Criminal Record

[redacted]

E.6.1. Criminal Records are verified by fingerprints which are provided by the requesting departments. (See E.9)

Analyst:

(a) Review the results of the fingerprint check:

- if a Criminal Record exists assess any relevance to the security assessment. (See attachment E.6.2.1.)

(b) In determining if a field enquiry and/or subject interview is needed the following points must be considered:

- [redacted]
-
-
-

- [redacted]
- [redacted]
- [redacted]

NOTE: Under section 748(3) of the Criminal Code - Unless it is a Pardoned Criminal Record, no person who is convicted of an offense under section 121, 124 or 418, has, after that conviction, capacity to contract with Her Majesty to receive any benefit under a contract between Her Majesty and any other person or to hold office under Her Majesty.

The offences referred to therein relate to:

Sec. 121 - Fraud Upon the Government
Sec. 124 - Selling or Purchasing Office
Sec. 418 - Selling Defective Stores to Her Majesty

E.6.2. Criminal Record Name Check (CRNC)

- checks may be conducted [redacted]
- CPIC information is restricted and is not to be disseminated beyond CSIS without proper notification to CPIC Services.

NOTE: A criminal record will not be released by the RCMP without validation from fingerprints.

E.6.3. Pardoned Criminal Record

REFERENCE: 1. Solicitor General letter dated 6 June 1988, file IP371-40

2. Letter from DG-OSS to RCMP 1 AUG 90 - IP 371-1

1. For handling instructions, see Pardoned Criminal Record Booklet.

2. The RCMP has been instructed to release to CSIS only those records for which a pardon has been granted where:

   (a) those offences are punishable by indictment
   (b) for "dual offences", those offences that appear to be of a serious nature or indicative of a pattern of behavior, i.e. five or more convictions for related offences.

NOTE: PCR can only be used with the authorization of the Solicitor General. Employees should be acquainted with Ministerial Directive - dated 8 June 1988.

E.7. Credit Bureau Checks

REFERENCE: 1. letter from DG Security Screening, 30 July 1987, IP371-1
2. memo DDG Security Screening to DDG Records, 12 July 1989, IP371-1

E.7.1. Departments are responsible for conducting a credit check for all security clearance requests. Where the department has not undertaken such a check, CSIS will do so.

NOTE: Credit Bureau information is only an indicator of an individual's financial status. All information must be corroborated.

E.7.2. Analyst:

(a) Ensure credit report is that of the file subject and assess overall credit rating, [redacted]

(b) [redacted]

(c) [redacted]

(d) [redacted]
(e)

E.8. Out-of-Country Field Investigations

E.8.1. Out-of-country field enquiries shall be conducted:

(a) Where facilities exist to conduct enquiries on [redacted]

E.8.2. Out-of-country <u>records checks only</u> shall be conducted:

(a) [redacted]

(b) when field enquiries are not available (see World Index).

E.8.3. When out-of-country field enquiries are required but facilities do not exist, [redacted]

E.8.4. Fingerprint checks may be conducted abroad where facilities exist and when requested by the department concerned.

E.8.5. When requesting Security/Criminal checks [redacted]

E.9. FINGERPRINTS

REFERENCE: 1. International Industrial Agreements (see SSC, Industrial Security Manual)
2. DDG memo, IP371-1, 21 Feb 90

E.9.1. Processing fingerprints:

(a) Fingerprint deemed unreadable by the RCMP

(1) Return fingerprints which are not processed by the RCMP because they are unreadable to the requesting agency so they can be retaken.
(2) If the prints are unreadable after three attempts request a CPIC check and provide the requesting agency with an incomplete assessment, with appropriate explanation in the limitations section.

(b) Refusal by subject

(1) Advise the DSO and return the documentation with an explanatory memo. [redacted]

NOTE: Refusal is not an acceptable reason for an individual not to provide fingerprints therefore an assessment will not be provided.

(c) Medical or Other Legitimate Reasons Other Than Refusal

(1) Provide an incomplete assessment with an appropriate explanation in the limitations section.

NOTE: The requesting agency should provide documentation outlining the reason(s) fingerprints could not be obtained.

(d) Out-Of-Country Checks
- except as provided for in E.8.4.,

(1) [redacted]

NOTE: Consult the World Index.

(e) Recent Criminal Offence

(1) The RCMP require resubmission of fingerprints to confirm the existence of a criminal record on a subject who requires an upgrading or updating of a security clearance and who may have been recently charged with a criminal offence.

(f) [redacted]

E.9.2. Return to DSO

Fingerprints are to be returned to requesting agency, with the [redacted] or the brief, as the case may be.

E.10. Court Proceedings

(a) Analyst:

Do not task the field to conduct a subject interview if the subject has been charged with a criminal offence and the matter is still before the courts. This would not apply if the subject had been convicted and the matter was under appeal.

[redacted]

NOTE: In exceptional circumstances, the sector manager may authorize interviews with subject who is charged with criminal offence.

(b) Field Investigators:

If, during the course of routine investigations, you discover subject has been charged with a criminal offence:

1. do not conduct subject interview
2. [redacted]
3. continue with investigation and inform HQ of the results.

(c) Analyst: Upon receipt of the field report:

1. assess information
2. request further investigation if necessary
3. consult with Unit Head, [redacted]
4. provide an assessment to requesting department, [redacted]

ATTACHMENT E.6.2.1.

DEFINITION

TERMS CONCERNING CRIMINAL CONVICTIONS

*(1) Discharge

At a preliminary inquiry, the presiding justice must determine whether there is any evidence which, if believed, could result in a conviction. If there is such evidence, the accused is ordered to stand trial. If there is no such evidence, the accused is "discharged" (see section 548 of the Criminal Code).

Neither disposition is a finding on the merits of the charge facing the accused. An accused who has been discharged has not been acquitted. An accused who has been ordered to stand trial has not been "convicted" - he continues to benefit from the presumption of innocence until the final disposition of the charge.

*(2) Absolute or Conditional Discharge

Pursuant to section 736 of the Criminal Code, where an accused pleads guilty or is found guilty of certain offenses, the court may, if it considers it to be in the best interests of the accused and not contrary to the public interest, instead of convicting the accused, direct that the accused be discharged absolutely or on conditions prescribed in a probation order. If an accused breaches the terms of the probation order, he may be brought back before the court which can formally enter a conviction and imposed sentence in respect of the offense for which a discharge was originally granted.

The discharge provisions of the Criminal Code enable a court, in appropriate circumstances, to dispose of a case without registering a conviction, while the accused has admitted guilt or has been found guilty, he is spared the stigma of a conviction. For the purpose of section 736 CCC, the accused is deemed not to have been convicted of the offense for which the discharge is granted. As a result, a person who receives a discharge may truthfully answer "no" to the question of whether he has been convicted of a criminal offense. Notwithstanding this, an automated file will be held with the RCMP, to certify the existence of the discharge.

Recent amendments to the criminal records act now forbid the disclosure of a discharge record or its existence without the prior approval of the minister:

- if 1 year has elapsed since an absolute discharge has been granted;

- if 3 years have elapsed since a conditional discharge has been granted and its conditions have been met.

A person who receives a discharge is no longer required to request a pardon, and the commissioner of criminal records shall remove all references to a discharge from the automated criminal conviction records retrieval system maintained by the RCMP on the expiration of the relevant period referred to previously.

(3) Suspended Sentence

There is conviction, however sentence is suspended for certain length of time; there may be a criminal record but the sentence does become a public record.

(4) Probation

Individual is convicted and sentenced to a period of supervision under a probation officer, which may or may not be preceded by a term of incarceration. Terms of probation vary widely and may include such conditions as abstinence from drugs or alcohol, avoidance of certain people, etc.

(5) Parole

Individual is released from incarceration early after serving a minimum of 1/3 of the sentence. The period of parole will equal the remainder of the sentence and be supervised by a parole officer under certain conditions similar to those mentioned under probation.

(6) Stay of Proceedings

There are two types of "stays".

The first type of stay is one entered in the absolute discretion of the Attorney General (i.e. the prosecutor). Sections 579 and 795 of the Criminal Code allow the Attorney General to enter a stay at any time after criminal proceedings are commenced and before judgement. The proceedings may be recommenced at any time within one year of the date on which the stay was entered. If the proceedings are not recommenced within that period, then the proceedings are deemed never to have been commenced.

The second type of stay is one entered by the court itself. A judge may stay proceedings where compelling an accused to stand trial would violate those fundamental principles of justice which underlie the community sense of fair play and decency and

to prevent the abuse of a court's process through oppressive or vexatious proceedings.

Either type of stay has the effect of suspending a criminal charge before a decision has been made on the merits of the charge. As the proceedings have not reached the point where the accused has been convicted, the accused is entitled to be presumed innocent of the charge with respect to which a stay of proceedings has been entered.

(7) Dismissal

Court proceedings are a matter of public record. This term is generally used to describe the judicial order which finally disposes of a charge in favor of the accused. A charge may be dismissed at a preliminary inquiry when a judge ordered that the accused be discharged. A charge may be dismissed at trial following entry of a verdict of acquittal.

*(8) Pardon

Arrest and conviction all wiped clear and expunged totally. Refer to the Pardon Criminal Record Booklet.

*(9) Acquittal

Abolishes criminal conviction but carries with it public record.

A verdict of acquittal is a finding, made on the basis of evidence adduced at trial, that the accused did not commit the offense with which he was charged. It reflects the application of the criminal burden of proof (i.e. beyond a reasonable doubt) to the evidence admitted at trial.

* Subject can correctly say on PSCQ that he has <u>not</u> been convicted of a criminal offense; however, he may have a record which can be accessed by police and security authorities.

ATTACHMENT E.7.2.1

CREDIT RATING - GUIDELINES

BANKRUPTCY

1. If the bankruptcy is:
   a) Outside five year period, discharged, and good current credit rating - no action necessary.
   b) Outside five year period, discharged, and no indication of current credit rating (or a number of R4s, R5s, etc.) - request subject interview.
   c) Inside five year period - request subject interview.

   NOTE: The Bankruptcy Act, available through open information section, provides detailed information on the bankruptcy process in Canada.

SUITS & JUDGEMENTS

1. If there exist one or two suits or judgements:
   a) Outside five year period, in conjunction with good current credit rating (taking into account amount involved in the suit) - no action necessary.
   b) One or two outside five year period, along with questionable current credit rating (i.e. R4s, R5s, and R6s); DO SERVICE 12 and if conditions remain constant, request subject interview.

2. If there exist more than two outside five year period - request subject interview.

3. If there exist one or more within 5 year period - request subject interview.

4. If one or more suits are still pending (no judgement) - conduct a field investigation and if necessary a subject interview.

LIENS

1. In the absence of a poor credit rating determine number of liens and total amount in comparison to subject's employment (estimated income).

   NOTE:
   a) Mortgages are not listed as a lien on a Credit Bureau printout.
   b) Liens in themselves are not necessarily indicative of a financial problem.

2. If the amount of the lien does not appear to be realistic in comparison to the subject's salary, request a subject interview.

3. If all liens are current (i.e. within past year) and registered at different financial institutes - request a subject interview.

4. If liens are exclusively with Finance Co.'s and not Banks - request a subject interview.

5. If subject has three or more substantial liens in conjunction with a shaky rating (i.e. R3s and R4s) - request subject interview.

COLLECTIONS

1. If there has been one collection within five year period in conjunction with good credit rating - no action necessary - the amount should be considered.

2. If there have been two or more collections outside five year period (consider amount) with good credit rating - no action necessary.

3. If there is poor credit rating - request subject interview.

4. If there have been two or more collections inside five year period - request subject interview.

F. FIELD TASKING AND INVESTIGATIONS - GENERAL

REFERENCE: 1. memo dated 27 February 1986, IP371-1
2. memo dated 14 April 1987, IP371-1
3. telex dated 25 April 1988, IP371-1

F.1. General

F.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 a decision to undertake an investigation.

F.1.2. The investigational and analytical components of the security screening process are crucial for the quality of assessment of a person's loyalty and related reliability. It is important that analyst and investigator be acquainted with the Guide to Field Investigators and Headquarters Analysts.

F.2. Headquarters Analysts

F.2.1. In tasking the field to conduct an 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 the sector manager.

F.2.2. Specify to the regional office the type of investigation (Level 3 or Level 1 or 2 "for cause").

Provide:

(a) A copy of the PSCQ for the subject with a legibly completed signed Consent form (TBS/SCT 330/58);
(b) any trace information including [redacted] check results,
(c) the results of Credit Bureau check(s), including Service 12;
NOTE: When a subject interview is being requested of a district/region outside the district/region where the serious crime(s) was committed, [redacted]

[redacted]. This could be done by simultaneously tasking the two regions concerned [redacted]

(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);
(i) name of analyst and Unit number.

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

F.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 investigating Regions.

F.2.4. When a report is received, review 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.

F.2.5. An interview of the subject is warranted:

(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 H.3 and H.4)

F.2.6. In tasking the field with update requests, normally only the period since the last recommendation to the Department should be tasked for investigation.

F.3. Investigator

Refer to Appendix L.10 - A Guide to Field Investigators

F.4. Individuals in Sensitive Institutions

These guidelines are pursuant to the "Conduct of Investigations" policy and provide direction on the level of authority required for security screening investigations involving individuals in sensitive institutions.

1. Regional DGs must advise the DDO whenever a security screening investigation is to be conducted involving senior public officials, prominent persons or where there is potential for public controversy, in which case the DG OSS should also be advised. The following are senior public officials:

   (a) the Governor General, lieutenant governors, legislators of political institutions at the federal level, provincial premiers, the Clerk of the Privy Council, and all persons who are heads of federal agencies and departments, such as Deputy Ministers and Presidents of various boards.

2. All other security screening investigations, including contact with the following individuals, may be conducted without advising the DDO:

   a) legislators of political institutions at the provincial and municipal level, persons in executive positions in the offices mentioned in 1 (a), such as Chief of Staff, Executive Assistant, Press Secretary;

   b) the registrar and professors of academic institutions, members of the media, members of the clergy or other persons officially representing a religious institution, a person acting in an official union capacity, and members of the judiciary.

F.5. DISCLOSURE OF LAW ENFORCEMENT INFORMATION

(a) PROCESSING CSIS ACT SECTION 19(2)(a), (b), (c) AND (d) INFORMATION

Paragraph 19(2)(a) of the CSIS Act, gives the Service discretion to disclose incidental information obtained in the performance of its duties and functions, if the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province.

(b) INVESTIGATOR

Refer to Chapter IV.1.G (OM) for the reporting and disclosure procedures for information that relates to law enforcement as specified in Section 19(2)(a) of the CSIS Act.

(c) HQ ANALYST

In accordance with Chapter IV.2.G (OM), prepare appropriate correspondence for signature of the sector manager.

G. SECURITY ASSESSMENT

REFERENCE:
1. IP371-1 memo dated 2 February 1989
2. IP371-1 dated 24 November 1988
3. IP371-1 dated 06 February 1991, to DDG Records
4. IP-371-1 memo to file from DG-OSS dated 26 November 1991

G.1. [redacted]

PSS has been delegated full responsibility for processing requests for level I and II, priority "D" and "E", and all supplementals for levels I and II, where there is no trace information. (Refer to Chapter C. for further explanation).

G.2. Analyst

G.2.1. For those requests which have not been processed by [redacted], ensure that there is sufficient information to make a complete analysis and an assessment of the subject's loyalty and related reliability.

The following must be considered:

(a) [redacted]
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
(j)

[redacted]

G.2.2. When there is no derogatory information, process clearance requests, [redacted]

G.2.3. Where derogatory information exists and is deemed not to represent a potential security concern, you may elect to proceed [redacted] after consultation with your Unit Head, with appropriate comments in the "Comments" portion.

G.2.4. In the following cases submit file to the [redacted] through Unit Head:

(a) when derogatory information exists which may have an effect on an individual's security clearance;
(b) when advice or cautionary note to the department is required;
(c) all cases where revocation or denial are contemplated.

G.2.5. Unit Head

(a) conduct quality control to ensure signing authority chart is respected;
(b) refer all proposed denials to the Sector Manager.

G.3. Allegations of Security Concern

Analyst

G.3.1. When allegations or derogatory information is received [redacted]

G.3.2. Assess the allegation in light of its seriousness and consider the source to determine if the security concern is founded and whether it has been previously

reported. Discuss each incident with the Unit Head to determine if the file should be revisited or wait for the subject's update.

G.3.3. If the allegation does not appear legitimate, place it on file with a note indicating that no action was taken.

If you judge the allegation to have a possible bearing on the security clearance of the individual, consult with your supervisor. If the concern is valid, initiate field enquiries, and:

(a) [redacted]

(b)

(c)

Upon receipt of the field report, assess the information:

(a) if the allegation is resolved, place a note to file clearly stating the reasons for your judgement;
(b) after field enquiries, if the allegation is not resolved, consult with your supervisor, and transmit to [redacted] for an assessment.

Advise the DSO of the results either by [redacted] or detailed brief.

If the allegation:

(a) has been previously reported - place new information on file and note the fact that the allegation had surfaced previously and what action had been taken to deal with the concern;
(b) has not been reported - if the allegation is judged to have a bearing on the security clearance of the subject, make a notation on the file accordingly, clearly stating the reasons for your judgement and consult with your supervisor.

G.4. Security Assessment of Juveniles

REFERENCE: 1. letter DG FSS to TBS, 7 November 1988, IP371-1
2. [redacted]
3. IP371-1, [redacted]

G.4.1. Upon receipt of the PSCQ package, [redacted] will ensure request for security assessment on persons less than 18 years of age is accompanied by a consent form co-signed by a parent or guardian.

(a) If this consent is not included return PSCQ package.

G.4.2. Once the consent form is in order, conduct the necessary indices checks.

G.4.3. When requesting a field or subject interview on a person 18 years or less who has a criminal record under the Young Offenders Act (YOA):

(a) [redacted]

(b)

G.4.4. Although biographical information on the PSCQ is only provided back to the age of 16 years, investigators may make enquiries as far back as required.

G.4.5. A parent or equivalent adult should be present at any subject interview.

G.4.6. The final assessment for non-adverse responses must include the appropriate caveat (see D.7.3).

G.4.7. Where adverse information has been raised, the file should be forwarded [redacted] for a detailed assessment.

G.5. Upgrades/Downgrades

G.5.1. For upgrades from Level 1 to Level 2 within 12 months:

(a) Upon receipt of the department's request for an upgraded clearance, review the file to ascertain the date the last [redacted] was provided before recommending Level 2.

G.5.2. For upgrades from Level 1 to Level 2 over 12 months:

(a) Upon receipt of the department's request for an upgrade with new documents, conduct Credit Bureau, criminal record, if applicable, and CSIS checks.
(b) If the information on the file is non-derogatory, recommend Level 2.
(c) If the information is derogatory, [redacted] and advise the requesting agency of the delay.

G.5.3. For upgrades from Levels 1 or 2 to Level 3:

(a) Upon receipt of the department's request for an upgrade with new documents verify the dates of the last checks. If [redacted], ensure the department has conducted a Credit Bureau (optional), criminal record check. CSIS to conduct CSIS checks.
(b) Task the field for a 10 year background check, or to age 16 whichever comes first.
(c) If foreign checks are required, advise the department by letter of the delay.
(d) Once the field investigation is completed, provide [redacted] or request a brief be prepared to the requesting agency.

G.5.4. If a notification of downgrading is received when a field investigation is still in progress, cancel the field inquiry immediately, and conduct appropriate checks.

[redacted] ANALYST

G.5.5. (a) Carry out standard verifications to ensure all requirements have been met.
(b) If a file requires more information for the purpose of preparing a security assessment, task the field accordingly via the portfolio Unit Head.
(c) Once file is complete, determine whether adverse information is security-related and pertains to the subject.
(d) If the information is not security-related, return file to Unit concerned for [redacted].
(e) If the information is security-related prepare an assessment with full rationale including the effect that any adverse aspects could or should have on the subject's security status taking into consideration any mitigating factors.

(f) Provide a recommendation to grant, deny or revoke a security clearance.

(g) [redacted]

(h) Submit for consideration and signature. (see Signing Authority Chart).

(i) If the recommendation is to deny or revoke a security clearance, prepare a case brief suitable for consideration by senior management and Legal Services.

G.6. Quality Control Program

REFERENCE: Memo 91-10-22, IP-371-42

G.6.1. Regional Quality Control

Under the responsibility of the [redacted], the Regions will select files at random for quality control purposes (Ottawa, Toronto and Quebec Regions should conduct two investigations per month, while the others, Atlantic, Prairie and B.C. Regions, should conduct one a month).

The Regions will submit, through the [redacted], a status report to the DG OSS once a year, no later than March 15th. This report must contain the file number, the month in which the investigation was conducted and comments on the results, ie. whether the original investigation was conducted according to established policies and procedures. The files selected for quality control will be noted, and the annual list pa'd to IP-371-42.

G.6.2. Investigator Responsibilities

Before conducting a quality control investigation, contact the subject in order to obtain his/her approval and explain the investigation is for quality control purposes.

[redacted]

[redacted]

3. that the original investigator neither omitted nor added any comments which might have had an impact on the subject's security clearance.

NOTE: Any irregularity uncovered during a quality control investigation is to be reported immediately [redacted] to the DG Security Screening at HQ.

G.6.3. HQ Responsibilities

Unit Head:

1. Each month, select at random four files (regardless of the clearance level) from each of your analysts for the purpose of ensuring all aspects of security screening policy & procedures have been met. (Once the automated program [redacted] is implemented a computer program will make the selection randomly.)

2. Ensure all the required indices checks were performed; appropriate field and out of country tasking, and retasking where appropriate, occurred; and an appropriate recommendation was provided to the client department.

3. Make a notation on the file indicating it was subjected to a quality control exercise. As well, for tracking purposes, the list of the files reviewed must be PA'd to the Quality Control main file: IP-371-42.

4. Bring to the immediate attention of the Section Manager any irregularity uncovered during the quality control exercise.

Section Chief:

1. Is responsible for the smooth functioning of the HQ and Regional Quality Control Program for the departments he/she administers.

2. When irregularities are surfaced, take corrective measures.

G.7. Incomplete Assessments

G.7.1. Criteria for incomplete assessments:

(a) for inadequate coverage [redacted]

[redacted]

(b) Out-of-country checks

[redacted]

(c) Lack of adequate source coverage or lack of cooperation from subject of investigation

- ensure that all avenues of investigation have been exhausted.

- determine if there is sufficient information at hand, both qualitatively and quantitatively, to make an informed recommendation.

(d) certain indices checks were not conducted in conformity to the GSP i.e. a CRNC was done for Level 2, where a fingerprint check should have been conducted for a new request.

G.7.2. Recommendation

When preparing an assessment, the analyst should:

- prepare [redacted] with a positive recommendation, if the period missing is of little significance [redacted] An explanation should accompany the [redacted]
- prepare [redacted] with a positive recommendation, although [redacted]
- prepare [redacted] with an incomplete recommendation, [redacted] An explanation should accompany [redacted].
- send the file to [redacted], if [redacted]
- provide an interim to departments, if the out-of-country checks will be delayed.
- send the file to [redacted], if [redacted]
- refer all other situations to the Unit Head, who may consult with [redacted]

G.7.3. Signing Authority

(a) Analyst

In consultation with the Unit Head, the analyst may sign off [redacted].

(b) Unit Head

Refer those cases which require a detailed brief to [redacted].

H. SPECIAL REQUESTS

H.1. Airport Restricted Area Access Clearance Program (ARAACP)

REFERENCE: 1. Message ISS/3509/172 dated 87-11-30 on IP371-1 Implementing the ARAACP in September 1987
2. File IP375-67

H.1.1. Any person requiring access to restricted areas in an airport must have a Level 1 security clearance.

H.1.2. The Personal History Form (PHF) is a truncated version of the PSCQ in that:

(a) CSIS indices checks are done [redacted]

(b) the time period [redacted]

(c) [redacted]

(d) there is no listing for relatives or character references. (See also Chapter E.3.2.)

H.1.3. Upon receipt of the PHF, the analyst must ensure [redacted] checks are conducted if the subject [redacted]

1. [redacted]

2. [redacted]

H.1.4. When security concern exists, a field investigation and/or a subject interview will be undertaken.

H.1.5. Foreign checks may be conducted in cases where information indicates [redacted]

H.1.6. Responses to the client department must indicate the Level I clearance is a truncated version by including the appropriate caveat. (see D.7.3.)

H.1.7. If the subject has resided outside Canada [redacted] response is provided to the department with the appropriate caveat. (see D.7.)

H.1.8. Assess the file and provide an assessment in accordance with the established procedures. (See chapter G)

H.2. Ministry of Foreign Affairs and International Trade (MFAIT)

REFERENCE: 1. IP371-1
2. IP371-4
3. MOU between CSIS and MFAIT
4. [redacted]
5. CULLEN-COUTURE agreement

H.2.1. Foreign Service Officer (FSO)

(a) FSO are identified by the department on the top of the PSCQ. These include CIDA personnel and Quebec Immigration officers posted abroad.

H.2.2. FSO Updates

(a) MFAIT will on occasion request an updated Level 3 for a FSO with recent postings abroad or currently serving abroad, and specifically request Records checks only. "RECORDS CHECKS CANADA ONLY" will be stamped on the top of the page one on the PSCQ and should be processed like a level 2 request.
(b) MFA is to conduct credit and CRNC checks. CSIS to conduct indices check and if no derogatory traces are found, provide [redacted].

H.2.3. Subject Interviews of Employees Posted Abroad

(a) If a subject interview is required prior to providing a security assessment, the following three options can be utilized depending on the gravity and urgency of the situation:

1. consult with MFAIT to ascertain if the subject can return to Canada for the interview;
2. [redacted]
3. [redacted]

(b) Ensure MFAIT is aware of our concern.
(c) [redacted]

NOTE: ROTATIONAL STAFF
On occasion a Level 3 request will be received with a cover stamp of "ROTATIONAL EMPLOYEE". An interim Level II recommendation should be issued pending the completion of field enquiries, provided no adverse traces surface.

H.2.4. NATO Clearances

(a) MFAIT will provide a covering letter with requests stamped NATO;
(b) process "NATO Restricted" and NATO Confidential" as Level 1, "NATO Secret" as Level 2, and "COSMIC Top Secret" as Level 3;
(c) [redacted]

H.2.5. Locally Engaged Staff (LES)

(a) "Locally Engaged Staff," are not Canada-based, they may occupy either a program or support position in our missions abroad, and they fall within one of the following six categories:

1. A national of a country with which the Service has established security and intelligence liaison channels [redacted] SLO in Posts conduct the necessary security checks to determine whether the LES could be considered a threat under section 12 of the Act;
2. a national of a country with which the Service does not have established security and intelligence liaison channels. The Service is usually not in a position to offer meaningful comment;
3. a national of a country described above but who has lived in Canada for a significant period of time;
4. a Canadian born resident, and perhaps citizen of a country described in (a) or (b) above;
5. a nationalized Canadian citizen or Canadian born spouse of a Canadian-based staff member; and
6. a foreign citizen and foreign born spouse of a Canada-based staff member.

[redacted]

H.2.6. Security considerations and procedures for clearing LES employees must take into account [redacted] and whether the Service can legally respond to clearance requests received from the department [redacted]

H.2.7. Summary

(a) [redacted] the responsibility of Mission Security Officers abroad, who conduct the appropriate criminal and security checks through Field and Liaison (CSIS).
(b) If a security clearance is requested EAITC will forward complete GSP documentation to us.
(c) Checks in Canada generally do not apply; we still conduct record checks but a threat assessment is based on the LO's response.
(d) CSIS will provide to MFAIT the results of the enquiries conducted abroad.

H.3. Department of National Defence

REFERENCE:
1. DND letters to the DG Security Screening dated 5 December 1984 and 17 June 1985, file IP375-8;
2. correspondence relating to DND screening requests dated 16, 20 and 22 February 1989, file IP371-1-3;
3. Memorandum of Understanding - DND dated 16 August 1989, file IP371-1;
4. Social Insurance Number T.B. Submission IP405-29 dated 23 June 1988

H.3.1. All DND requests are conducted [redacted]. For those requests which generated a "hit", DND will submit to CSIS a full PSCQ package, for normal processing.

H.3.2. ANALYST

Where DND has submitted a full PSCQ package:

1. Assess CSIS trace information;
2. Initiate the out-of-country checks and/or field enquiries, if necessary;

3. Upon receipt of favourable foreign checks and when there is no reportable trace, prepare an [redacted] to DND for Levels 1 and 2. Level 3, only, to be signed by Unit Head.
4. Trace information is to be forwarded through the Unit Head to [redacted].
5. If necessary a joint subject interview with both CSIS and DND present may be requested.

H.4. Royal Canadian Mounted Police

REFERENCE: 1. MOU between CSIS and RCMP dated 22 August 1989
2. Ministerial Directive
3. Correspondence on IP371-1 and IP375-5-1

H.4.1. No "HIT" RCMP checks are handled by [redacted] and Security Screening [redacted]

H.4.2. ANALYST

1. Initiate necessary out-of country indices checks.
2. Initiate an out-of-country field investigation, if necessary, consulting with the RCMP Departmental Security Unit Head prior to initiating any action.

H.5. Applicants and Contracts

REFERENCE: 1. Executive Committee Decision (suitability for screening)

H.5.1. All CSIS applicants and contracts files are handled on a priority basis. (See OSS Annual Plan)

H.5.2. Level 1, 2 and 3 clearance for CSIS applicants and contracts are handled in the usual fashion, except for the following:

(a) [redacted]

1. Conduct indices checks [redacted]
2. Attach pink file jacket to file to identify the file as a CSIS applicant.
3. Identify CSIS fingerprints form as such and forward form to RCMP.

(b) [redacted]

1. Hand deliver the file and fingerprints to the unit concerned.

(c) Internal Security

1. Conduct the security interview of CSIS applicant.
2. When any derogatory information is surfaced provide it, without delay, to Security Screening Branch so that the field can be tasked accordingly.
3. Conduct a second subject interview at the request of Security Screening Branch when adverse information is obtained during the field investigation and provide a detailed report to HQ Security Screening Branch.

(d) Analyst

1. Conduct [redacted] checks on applicant [redacted]. If these checks produce trace results and if there is information which requires a headquarters operational evaluation; we must beforehand communicate our research results to Headquarters Internal Security. Only one written report (Internal Security and Security Screening) must be sent to [redacted]. The section (Internal Security or Security Screening) which receives the desk response must immediately forward a photocopy of the response to the other section.
2. If any derogatory information is surfaced by Internal Security task the field accordingly.
3. If any derogatory information is surfaced by the field, you may provide Internal Security with the details and task them to conduct a second security interview to address our concerns.

NOTE: When an interview of the subject is warranted, in some cases it may be more appropriate to task the Security Screening investigator to conduct the interview.

(e) Field Investigators

1. Provide Personnel Services with a suitability report except in the case where the candidate is applying for corps of commissionaires employment, the suitability report must be sent to Headquarters Internal Security under the file number [redacted]-name of subject.

2. If a subject interview is warranted advise HQ Security Screening Branch of your concerns.

[redacted]

3. When submitting your reports, use the following introductions:

Security clearance report submitted to Security Screening
This report is submitted at the request of the Director General, Security Screening, CSIS, to provide a security assessment, in relation to the individual's loyalty to Canada and insofar as it relates thereto his/her reliability. Its use is intended to assist the Director General of Internal Security, CSIS, in the determination of whether to grant or deny a security clearance.

Suitability report submitted to Personnel Services
This report is submitted at the request of the Director General, Personnel Services, CSIS to provide a suitability assessment of the individual's candidacy for employment with CSIS. Its use is intended to assist in the determination of whether or not the individual would make a suitable employee for CSIS.

(f) Unit Head

1. Review all cases which contain derogatory information and ensure that it has been addressed to the fullest extent possible.
2. Ensure a suitability report is submitted when derogatory information exists to Personnel Services.
3. Maintain liaison with Internal Security and Personnel Services.
4. When derogatory information exists forward the file to [redacted]. Ensure that all reports are in the file (i.e. Internal Security report).

[redacted]

H.5.3. Limiting Statement

(a) Depending on the circumstances the following limiting statements can be added to the assessment form:

1. Recommend Level 3 pending results of foreign indices check.
2. Recommend Level 2 while enquiries are underway.

H.5.4. Source Protection

(a) In all cases where a security screening investigation report contains information of an adverse nature, [redacted], the analyst will ensure that the relevant documentation is placed in an envelope, sealed, placed on the file, and noted with the following:

"TO BE OPENED ONLY BY CHIEF, GOVERNMENT SCREENING (OR DELEGATE) OR CHIEF, [redacted]"

The file number and report number will also be written on the envelope.

H.6. Order In Council Appointments

REFERENCE: 1. Letter dated 17 June 1987, Clerk of the Privy Council IP371-1.

H.6.1. These guidelines govern the procedures to be followed in respect of pre-appointment background checks on Prime Ministerial appointees and other Order In Council appointees.

H.6.2. Requests are to be treated as an immediate priority and are received:

(a) by telephone, from the RCMP; or by fax to the analyst [redacted]

H.6.3. A designated analyst coordinates the processing and:

(a) informs the Unit Head of the requests;
(b) requests [redacted] to conduct [redacted] checks;
(c) distributes copies of the requests to analysts to have [redacted] checks conducted;
(d) transmits a copy by secure Fax to the Chief, [redacted] for an indices check.

H.6.4. If traces appear, either through [redacted] or [redacted] checks, the analyst must:

(a) consult [redacted] branch as required;
(b) summarize the information in a briefing note;
(c) the Unit Head will consult with the sector manager to determine if it is necessary to advise RCMP.

H.6.5. Once all the checks have been completed, and if they are favourable, the analyst provides the interim result to the RCMP by telephone. On those requests where checks reveal information requiring further assessment, the analyst advises the RCMP of the delay.

H.6.6. Upon receipt of the RCMP's written request, the analyst provides the favourable results by letter using the established guidelines, to the Commissioner of the RCMP.

H.6.7. In those cases where a decision has been made to brief the RCMP, the Unit Head forwards the request to the [redacted]

H.7. Ministerial Staff

REFERENCE: 1. Letter dated 5 February 1987 from Clerk of the Privy Council.

H.7.1. Security clearance requests for Ministerial Staff are to be answered within 48 hours of reception.

H.7.2. When a PSCQ identified as "Ministerial Exempt Staff" is received by Security Screening Branch, it is immediately hand-delivered to [redacted] for the appropriate checks.

(a) The fingerprints are sent to the RCMP stamped "Ministerial Staff 48 Hour Check". When verbal results are received, the file is delivered to the Unit Head responsible.

H.7.3. Once [redacted] checks are conducted by the analyst, the originating department is provided with a "No Reportable Traces" response for Levels 1 and 2, over the telephone or is advised that there will be a delay if derogatory information surfaces.

H.7.4. With non-derogatory checks the analyst must complete a [redacted] for Levels 1 and 2.

H.7.5. Should field enquiries be required, the analyst must initiate the enquiries on a priority basis.

(a) Upon receipt of favourable field enquiry results, the analyst informs the originator by telephone followed with an appropriate Notice of Assessment.
(b) If briefing is warranted, the file is delivered to the [redacted].

H.8. Departmental Security Officers

REFERENCE: 1. CSIS 26, dated 9 May 1989, file IP371-1-3.

H.8.1. Special guidelines govern the processing of security clearance requests for personnel employed or to be employed, as Departmental Security Officers (DSO), as well as their staff.

H.8.2. For requests in which the subject is a DSO or is a candidate for this position:

(a) Process file in the usual manner.
(b) Upon completion, forward the file to the [redacted].
(c) The brief is to be forwarded to the Deputy Head of the requesting agency.

H.8.3. For requests involving staff employed, or to be employed, with the DSO's office:

(a) Process file in usual manner.
(b) Place recommendation in a sealed envelope and direct to the personal attention of the Departmental Security Officer.

H.9. Foreign Security Screening
(Telex to Washington: IP 371-1-3 dated 91-01-14)

H.9.1. (a) All requests for Security Screening from Foreign Agencies will be reviewed to make certain that the requests are consistent without reciprocal arrangements and that the request is clearly within Sec. 15 of the CSIS Act.

(b) When conducting or analyzing Foreign Screening requests, the threshold test applied shall be consistent with GSP.

(c) CSIS will not conduct security screening interviews of subject on behalf of foreign states or institutions.

Prohibition of conducting subject interviews on behalf of a foreign department is not based on legal restrictions but rather on a bilateral agreement. The CSIS Policy stems from the following:

1. CSIS does not at the present time conduct, on a routine basis, subject interviews for Canadian Government security clearance requests. As a result it is difficult to justify providing this service for a foreign institution.

2. Enquiries made in Canada on behalf of foreign institutions/states are, as closely as possible, guided by the Canadian Government Security Policy. As a result it would be impossible to interview a subject, whether Canadian or not, for a position of trust with a foreign government based on our Canadian standards which may or may not be similar to those guiding the foreign state.

3. Other constraints to CSIS enquiries are:

a) [redacted]

b)

c)

d)

The definition of subject is meant to include: foreign nationals, locally engaged staff, and Canadian nationals.

[redacted]

(d) All information disclosed to Foreign Agencies shall be controlled by the appropriate Caveat. (see D.7.)

H.9.2. Procedures

(a) The analyst reviews all foreign screening requests to determine 'Canadian content' and to ensure that the action requested is consistent with GSP.

1. Liaise with SLO or Foreign Agency Representative in Canada if necessary to clarify any uncertainties.

2. If the request is urgent, [redacted] done by phone and the file is hand delivered to [redacted] for indices checks/file/SSRN creation and returned to analyst, by hand.

(b) 1. Review incoming request to determine and initiate the appropriate field tasking.

2. When the appropriate enquiries are completed, prepare the response to the requesting agency.

(c) 1. In all non-derogatory enquiries, select the appropriate brief format, complete by including the points requested by the agency and covered in the field enquiry. The Unit Head will sign all completed reports involving field investigations.

2. [redacted]

3. [redacted]

4. Consent Forms authorizing investigation by Canadian authorities, signed by the subject, are required by CSIS prior to conducting field investigations, credit bureau or other checks.

5. A subject must have resided in Canada and be

of, or have been at least 16 years of age while resident in Canada, before screening action can be carried out.

6. All requests resulting in serious derogatory information of a security concern will be the subject of a briefing response to the requesting agency by the [redacted]

7. All favorable responses will be signed by the Unit Head unless otherwise provided for.

8. All Analyst contact with Foreign Agencies outside Canada will be via an SLO (where one exists).

9. During field investigations, regional investigators will not reveal the specific purpose of the enquiry.

10. CSIS will not conduct enquiries to confirm or establish the following information:
a) [redacted]
b)
c)
d)
e)

11. The criminal record of a subject (or spouse, if requested) will not be released, other than to advise that further enquiries may be directed to the Royal Canadian Mounted Police or the appropriate police agency. In the case of a spouse or intended spouse, the existence of a criminal record will not be identified unless it is deemed to be of a significant security concern and relative to a subject's access to classified assets.

12. CSIS indices checks will be conducted on a subject, [redacted]. Other enquiries will be conducted only if requested and are in keeping with Attachment "1".

13. CPIC indices checks will normally be conducted on a subject [redacted]

[redacted]

14. Credit Bureau checks will only be conducted on subjects when so requested by a Foreign Agency and accompanied by a consent form signed by the subject.

H.9.4. Requests Usually Requiring Briefs or Telex Responses:

Country Codes:

[redacted]

H.9.5. (a) Requests Usually Requiring Stamp-Backs - Procedures

Country Codes:

[redacted]

H.9.6.

Country Codes:

[redacted]

[redacted]

(1) Review incoming requests to determine which areas require field investigation for the purpose of providing a CSIS security assessment.
(2) Prepare a Field tasking form and attach any related documentation.
(3) In all non-derogatory enquiries, select the applicable brief format, complete by including points requested by the agency and covered in the field investigation, Unit Head will sign completed typed reports and send to Mail Room where the report will be sent to the requesting agency in double sealed envelopes.
(4) All Briefs will contain Caveat no. 2, with the exception of [redacted]
(5) Derogatory field enquiries.

H.9.7. (a) Other Requests - Procedures

(1) [redacted]
(2)
(3)
(4)
(5)

H.9.8. Reporting of Significant Information - [redacted]

1. All requests resulting in the discovery of serious derogatory information should be reviewed and forwarded to the [redacted] for response.
2. [redacted]
3. [redacted]
4. In the case of other Foreign Agencies or Departments, the report will be forwarded via the CSIS SLO having country responsibility.

NOTE: Should further details be required concerning Foreign Screening consult the annex book.

H.10. Security Breaches

REFERENCE: 1. GSP (SPIN) 1991-06-19

1. In addition to those responsibilities and obligations placed upon the DSOs by the GSP,

   (a) All requests for assistance in the form of threat and risk assessments, or reports of security breaches should be directed to:

   Assistant Director
   Requirements and Analysis
   CSIS
   P.O. Box 9732
   Ottawa Postal Terminal
   Ottawa, Ontario
   K1G 4G4
   Tel.782-0243

SECTIONS I. AND J. CAN BE FOUND ON FILE "SSPM IMM ENGLISH"

THESE DOCUMENTS ARE AVAILABLE IN HARDCOPY ONLY.

K. REFERENCES

1. Charter of Rights and Freedoms
2. CSIS Act (See L.1.)
3. Access to Information Act
4. Privacy Act
5. Criminal Records Act
6. Young Offenders Act
7. Security Policy of the Government of Canada and Personnel Screening Standards (See L.2.)
8. Operations Manual - II.3 (Security Screening)
9. Operations Manual - II.4, II.6
10. Ministerial Directives, 1986, 1987, 1989 (See L.3.)
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
20. Criminal Code

WITH THE EXCEPTION OF L.10., THE FOLLOWING DOCUMENTS ARE AVAILABLE IN HARDCOPY ONLY.

L. APPENDIXES

- L.1. CSIS Act and Security Offences Act
- L.2. GSP Personnel Screening Standards - November 1990
- L.3. Ministerial Directives
- L.4. Signing Authorities Charts
- L.5. GSP (Automated Data Bank)
- L.6. [redacted]
- L.7. Forms
- L.8. DSO List and Departmental Numbers
- L.9. File Numbers (to follow)
- L.10. Guide to Investigators
- L.11. Pardoned Records Booklet
- L.12. World Index
- L.13. Sponsors - List of Countries
- L.14. Maps

APPENDIX L.10.

CSIS SECURITY SCREENING FIELD ENQUIRIES

- A GUIDE FOR INVESTIGATING OFFICERS -

JULY 1994

TABLE OF CONTENTS

DEFINITIONS

Source: Any medium or person that can provide information on someone who is the subject of a security screening investigation.

Subversion: An action designed to undermine a government and whose ultimate aim is to overthrow established ideas and values and bring about social collapse. It does not include legitimate dissent.

Subject: A person who is the subject of an investigation.

Loyalty: Loyalty concerns arise when the subject is engaged in, or may engage, in activities that constitute a threat to the security of Canada, within the meaning of the CSIS Act.

Reliability: Reliability concerns arise when the subject, because of personal beliefs, features or character, association with persons or groups considered a security threat, or family or other close ties to persons living in certain countries:

i) they may act or may be induced to act in a way that constitutes a "threat to the security of Canada"; or

ii) they may disclose, may be induced to disclose, or may cause to be disclosed in an unauthorized way, classified information.

Lifestyle and its components: An inquiry into the manner in which an individual lives, acts and thinks, and his or her motivating factors, such as discretion, honesty, stability and integrity, to determine whether the person is trustworthy with respect to the aforementioned factors.

Colleague: An individual who works with the subject and carries out similar duties.

Features of character: Specific features that distinguish an individual from another.

Peer:	A friend or acquaintance of the subject who is usually in the same age group and has a similar social background.
Security Assessment:	An assessment of an individual's loyalty to Canada and, insofar as it relates thereto, of his or her reliability as defined in section 2 of the CSIS Act.
Full Investigation:	An investigation that covers all the elements described in chapter F of the Procedures Guidebook.
Partial, limited or selective investigation:	An investigation in which the HQ analyst, after studying a file, covers only some of the elements described in chapter F of the Procedures Guidebook.
Neighbourhood inquiry:	An inquiry that consists in interviewing sources in the neighbourhood where the subject has resided during the period covered by the investigation.
Recommendation (regarding security clearance):	The recommendation for a level 1, 2 or 3 security clearance is based on an analysis of the investigation results, and is accompanied by pertinent comments for the department concerned, if necessary.
Corroboration:	The process of verifying the information received with sources who are acquainted with subject or who are able to confirm or deny an event or a statement involving the subject.
Immigrant:	A person who has applied to enter Canada for the purpose of settling in this country.
Landed Immigrant (permanent resident):	An immigrant who has been granted permission to establish his or her permanent residence in Canada.
Refugee:	Any person who has reason to fear persecution because of his or her race, religion, nationality, membership in a social class or political opinions, and who is outside his or her country of nationality.

Trace:	Any adverse information obtained that may relate to a threat to the security of Canada as defined in the Immigration Act, the Citizenship Act, or the CSIS Act.
Adverse Information:	Any information obtained during a security screening investigation that may constitute a threat to the security of Canada as defined in the Immigration Act, the Citizenship Act or the CSIS Act.
For cause:	The action to be taken, on the basis of available information, in order to continue the investigation.
National interest:	The national interest refers to the defense and preservation of Canada's social, political and economic stability, and thus the security of the nation.
Security clearance:	An assessment of the loyalty to Canada and, insofar as it relates thereto, the reliability of an individual.

A) GOVERNMENT SCREENING

1. Security Assessments

The Service's mandate for providing personnel security assessments to other Federal Government departments and agencies is set out in section 13 of the CSIS Act. Subject to the approval of appropriate Ministers, CSIS may also enter into arrangements authorizing the provision of security assessments for:

- provincial governments or departments;
- provincial police forces; and
- foreign governments, institutions, or international organizations.

The provision of security assessments for a large number of federal government departments and contractors represents a very demanding component within the overall mandate of the Service. Assessments entail forming a fair and accurate judgment of a person's loyalty to Canada, and of that person's reliability as it relates to loyalty. CSIS must comply with legislation, ministerial directives and policy which specify what a security assessment must address.

First, section 2 of the CSIS Act defines a "security assessment" as an "appraisal of the loyalty to Canada and, so far as it relates thereto, the reliability of an individual".

Second, the Appendix "D" of the Government Security Policy (GSP), a public document, sets criteria to be taken into account in making security assessments. This policy integrates "threats to the security of Canada" with loyalty and related reliability criteria, to effectively protect sensitive government information and assets. The GSP also provides criteria and procedures for the classification and protection of government information and assets.

Third, the "Ministerial Directive on the Provision of Security Assessments", issued in 1986, sets standards and guidelines to govern the provision of security assessments and related investigations pursuant to s. 13 and s. 15 of the CSIS Act.

2. Investigative Authority and Approved Investigative Techniques

Section 15 of the CSIS Act provides the authority for the Service to conduct such investigations as are required for the purpose of providing security assessments. The following are appropriate investigative techniques under Section 15:

1) searching CSIS classified and open information data banks,

2) criminal records name checks,

3) credit bureau checks,

4) [redacted]

5) [redacted]

6) inquiries conducted with foreign agencies,

7) interviewing the subject.

The decision to [redacted] is shared between HQ and the Regions. In most cases, the decision to conduct such interviews will be made by HQ on the basis of available information and consultation with [redacted] analysts. It is possible, however, that an investigator tasked to conduct an interview of a subject would be aware of [redacted]

3. Field Enquiries

3.1 Purpose of Field Enquiries

Field enquiries are initiated for Level III security requests, and "for cause" on Levels I and II. The purpose of background Security Screening investigations is to supply the requesting government institution with a security assessment on persons proposed to occupy positions requiring access to classified information or assets. Adequate quantity and quality of information is provided by at least four sources, and usually six, and normally covers the last ten continuous years or to age 16 years, whichever comes first, for clearances at all levels.

3.2 Factors of Concern

The decision to grant or deny a security clearance is based primarily on the Service's recommendation concerning the individual's loyalty to Canada, as well as the individual's reliability as it relates to such loyalty.

A. Features Associated with Loyalty Risk

Security assessments on matters of questionable loyalty should reflect the "threats to the security of Canada" as defined in the CSIS Act. Normally, information questioning a subject's loyalty will surface in the initial check of CSIS indices. Nevertheless, investigators should be alert to any one, or combination of, the following indicators:

B. Features Associated with Reliability Risk

Information concerning an individual is assessed with respect to its nature and seriousness, surrounding circumstances, frequency, the willingness of participation, the person's age at the time of the

incident(s), and the degree of rehabilitation which has occurred since that time.

Attention must be given to the following:

[redacted]

A decision to grant or deny a security clearance must be based upon adequate information. Where such information does not exist, or cannot be obtained, a security clearance recommendation cannot be given.

The following list is meant as a guide in addressing features associated with reliability risks:

[redacted]

[redacted]

3.3 Conducting Field Enquiries and Interviews with Sources

Each security screening investigation is different and unique.

[redacted] In preparation and during an interview, an investigator:

1. should properly identify himself and explain the authority and purpose of the screening interview.

   Normally the source need only be told that the subject has applied for a position with the Federal Government for which a security clearance is required. Discretion can be applied in those cases where the subject has already clearly indicated to the source the latter would be a character reference for a particular job application.

   All necessary forms, duly signed, should be readily available; the Personnel Security Clearance Questionnaire (PSCQ) and the subject's consent form. Internal Security Policy concerning the security of documents allows all investigators conducting Section 15 investigations to remove information from Service premises such as PSCQ or similar documentation at the "Protected" level. [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

7. [redacted]

8. [redacted]

9.

10.

Tape recordings of source interviews is prohibited.

4. Subject Interviews

4.1 Procedures

Subject interviews may be generated by HQ analysts for Levels I and II to clarify an indices trace. Depending upon the results of the subject interview, there may/may not be a need for a full or partial field investigation to obtain further corroboration. HQ may request that a field investigation be conducted prior to a subject interview in certain Level I and II cases where the trace information is of a more serious nature.

Initial Level III Requests

The field investigation should always be completed before the subject interview. This should ensure the investigator will be in possession of all available information at the time of the initial subject interview and thus avoid a requirement for a second subject interview.

The investigator, in consultation with his immediate supervisor, may decide when a subject interview is necessary to resolve doubts raised during the investigation. However, a second or third subject interview should only be carried out with the concurrence of HQ. HQ will advise, based on all available information, if the second subject interview is a necessity in order to arrive at an assessment of the subject's loyalty and related reliability. Attention to this procedure should help

to avoid potential complaints of harassment from individuals subject to repeated subject interviews.

Update Level III Requests

Field enquiries are no longer routinely conducted for level III updates. The Revised GSP (June 1994) requires departments to have in place a process to assess the individual's continuing reliability and loyalty. Where the results of the criminal or credit check (conducted by the department) reveal significant adverse information, departments are to conduct an interview with the individual to resolve any doubt prior to submitting the request to CSIS.

Departments must also conduct subject interviews for persons who will access SIGINT material. Departments should also conduct subject interviews for update requests, in order to manage the risk associated with conferring level III status without the benefit of a field investigation.

4.2 CSIS Applicants

For the same rationale, all subject interviews involving CSIS applicants, including the initial one, should be conducted by field investigators only after having the concurrence of HQ. CSIS applicants undergo several Personnel and Internal Security interviews and the HQ analyst is in the best position to determine if additional field subject interview is warranted.

HQ Internal Security (I.S.) maintains a close liaison with the HQ section responsible for CSIS applicants. Any information discovered during the I.S. interview that would impact on the field investigation will be forwarded to the Region immediately through the HQ OSS analyst. Regions conducting parallel investigations on the same subject can info the other Region with their report if trace information exists, however, this is to be an info copy only and HQ OSS must receive the original report.

4.3 Lawyers

The subject is permitted to have a lawyer or other person of their choice present during the interview.

4.4 Tape Recordings

The investigator may tape record the interview but only with the full knowledge and approval of the subject. Likewise, the subject can tape record with the interviewer's consent.

4.5 Consent

If, during the investigation and/or the subject interview, information comes to light that requires investigation or

clarification outside the purview originally provided on the consent form, the subject may be asked to give further permission to the investigator by completing the appropriate box on the consent form. This may involve a follow-up interview with a person whose information is normally seen as "privileged", e.g., a doctor, lawyer, psychiatrist, etc. If the subject consents, this person's name and the type of information to be revealed, e.g., medical, legal, should be entered and signed by the subject. HQ must be advised and the DDG OSS must concur prior to any special source interview subsequently taking place.

5. Reporting

There are two standardized formats to be used by all Regions in reporting to HQ on their case investigations. These formats are to be considered as guidelines to be followed in organizing and presenting information (see Appendix B).

APPENDIX "A"

1. Source Interviews

Source interviews must be individualized, but against this backdrop a number of possible questions are suggested. The list is neither all-inclusive nor inflexible; the questions are offered with the caution that they might not suit every situation or circumstance. Points to remember are:

1. [redacted]
2.
3.
4.
5.
6.

7. [redacted]

8. [redacted]

9. [redacted]

10. [redacted]

11. [redacted]

[redacted]

The Region may develop questions/models for use by their investigators, especially in the training of new personnel.

2. Topic Areas

The question areas which follow are provided for guidance and perspective, and should be adapted as needed. [redacted]

EMPLOYMENT

[redacted]

[redacted]

EDUCATION

[redacted]

NEIGHBOURHOOD

[redacted]

[redacted]

USE OF ALCOHOL/DRUGS

[redacted]

[redacted]

MENTAL OR EMOTIONAL STABILITY

[redacted]

MORAL BEHAVIOUR

[redacted]

SEXUAL LIFESTYLE

[redacted]

[redacted]

FINANCIAL RESPONSIBILITY

[redacted]

ORGANIZATIONS

[redacted]

LOYALTY

[redacted]

[redacted]

CRIMINAL HISTORY

[redacted]

SECURITY

[redacted]

CONCLUSION

Is source aware of anything which might preclude the subject from obtaining a security clearance?

3. Subject Interviews - Trace Information

Poor Credit Rating:

The investigator should be in possession of the Credit Bureau (CB) report [redacted]. A new CB report should be requested from HQ if [redacted] have elapsed since the CB report on file was obtained. After covering all loyalty/reliability factors and the subject has admitted to his credit problems, the investigator should question and report on:

-
-
-
-

[redacted]

The foregoing should enable the investigator to make an assessment of subject's current financial responsibility, whether it appears subject is living within his/her means, and whether or not subject's financial situation might be desperate enough to make him a potential target to abuse access to classified information or assets.

Sexual Lifestyle:

[redacted]

During a subject interview:

a) [redacted]

b)

c) [redacted]

Criminal Record(s):

Prior to conducting a subject interview for a criminal record, all relevant circumstances should be obtained from one or more of the following sources (depending on the seriousness of the offence):

- [redacted]

Criminal code offences for which the subject received a conditional or unconditional discharge from the court, are not required to be entered on the PSCQ as a criminal conviction(s).

[redacted]

Furthermore, the subject may be under the mistaken impression that the court gave a pardon and that no criminal record exists in relation to the offence. In the context of relatively minor Criminal Code offences, which were fully clarified with the subject, the investigator may inform the subject of the availability of the Criminal Pardon process (available through all Regional Offices of the National Parole Board).

The guidelines on the handling of Pardoned Criminal Records (PCR) are covered in the Procedures Guidebook Section L.11.

[redacted]

If the source (not the subject) is concerned about providing information surrounding a possible minor criminal offence which

may not have been reported to the police, the investigator can assure the individual the investigation/interview being conducted is concerned with security matters, not criminal.

[redacted]

CSIS Indices:

When files arrive at the Region [redacted] the applicable Regional Desk should be consulted. In a limited number of cases it might be advantageous to [redacted]. Prior to conducting the investigation, ensure [redacted] have been reviewed so the interviewer is fully aware of all aspects of [redacted]. Normally this should have all been completed by the HQ analyst in conjunction with [redacted]. If this has not been done and/or the HQ tasking instructions are not clear, contact HQ before proceeding with the investigation.

Prior to the subject interview, [redacted]

Joint Interviews With Other Agencies:

RCMP and DND may call on CSIS to attend one of their Security Screening subject interviews [redacted]

Subject Interviews - Level III Updates

Unlike interviews conducted for cause, these interviews should normally be conducted by departments. However, several departments have not yet established formal interview programs. The Service has offered to assist departments in these interviews, on a temporary basis, until such time as the departments are prepared to assume their responsibilities in this regard.

Departments have been informed that screening investigators will be conducting interviews on their behalf for level III updates. To help the investigator prepare for these interviews, the HQ analyst will review the previous field investigation and CSIS recommendation, and the results of the current CSIS, criminal and credit check. Satisfied that there are no traces to follow up, the analyst will task the region to "conduct an update interview on behalf of the department", and provide the region with the pertinent details/reports of previous investigations.

The investigator then proceeds with the initial contact of the individual to arrange an interview. It is imperative that the investigator mention at this time:

a) that this interview is an update interview, conducted on behalf of that individual's department, and the interview consists of standard questions which are routinely asked of all individuals;

b) the recent changes to the GSP (JUNE 1994) wherein field enquiries are no longer conducted for level III updates.

At the interview, the investigator should:

c) emphasize once again points a) and b);

d) review the PSCQ with the individual, to ensure the information is complete and accurate;

e) ask if there has been any change in her/his personal life, such as a separation, divorce, common-law relationship, etc. If the individual informs you of a same-sex relationship, ensure the

details of the partner are recorded. Given that the individual has informed you of this detail,

f) [redacted]

g) [redacted]

h) [redacted]

i) [redacted]

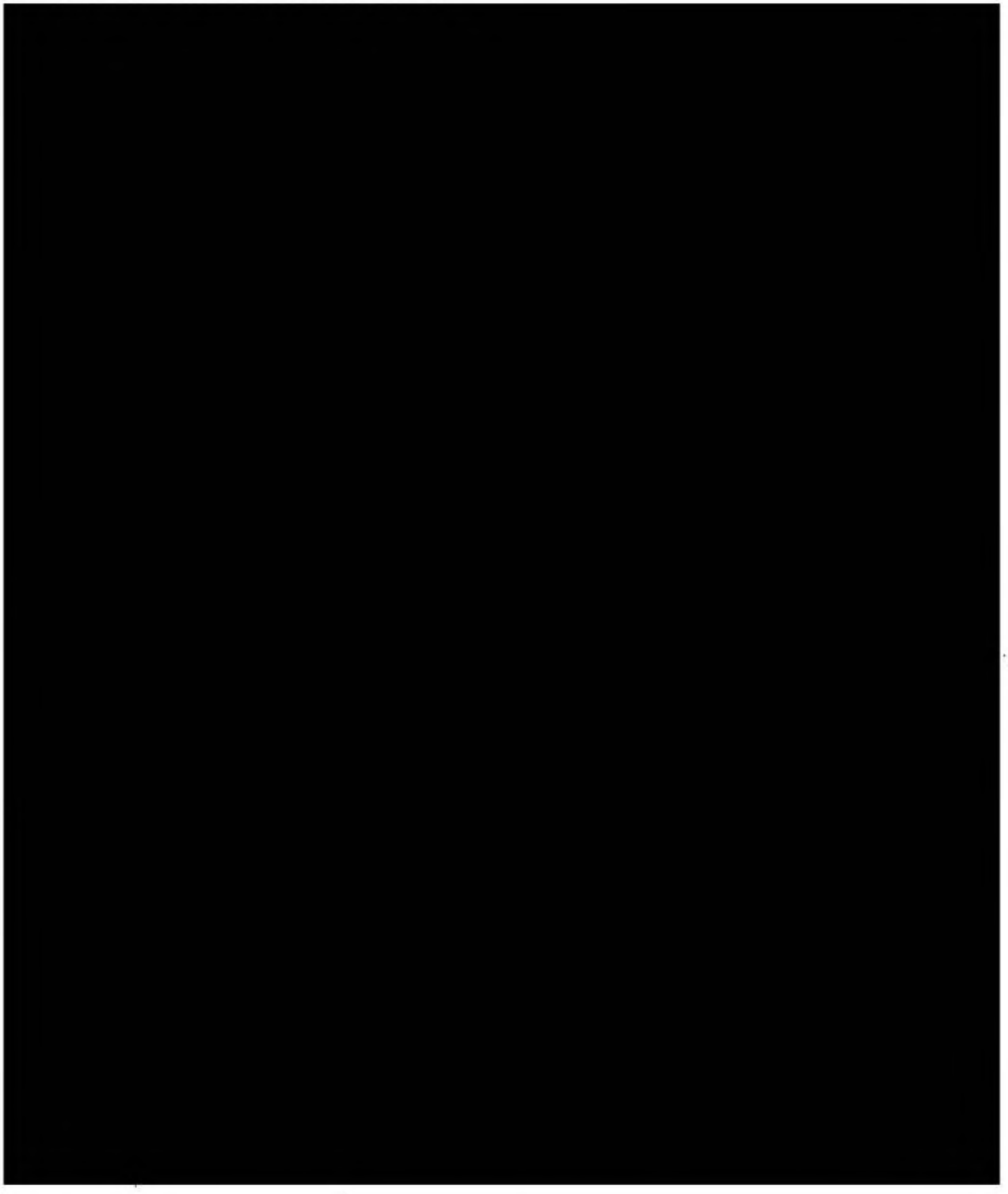
j) [redacted]

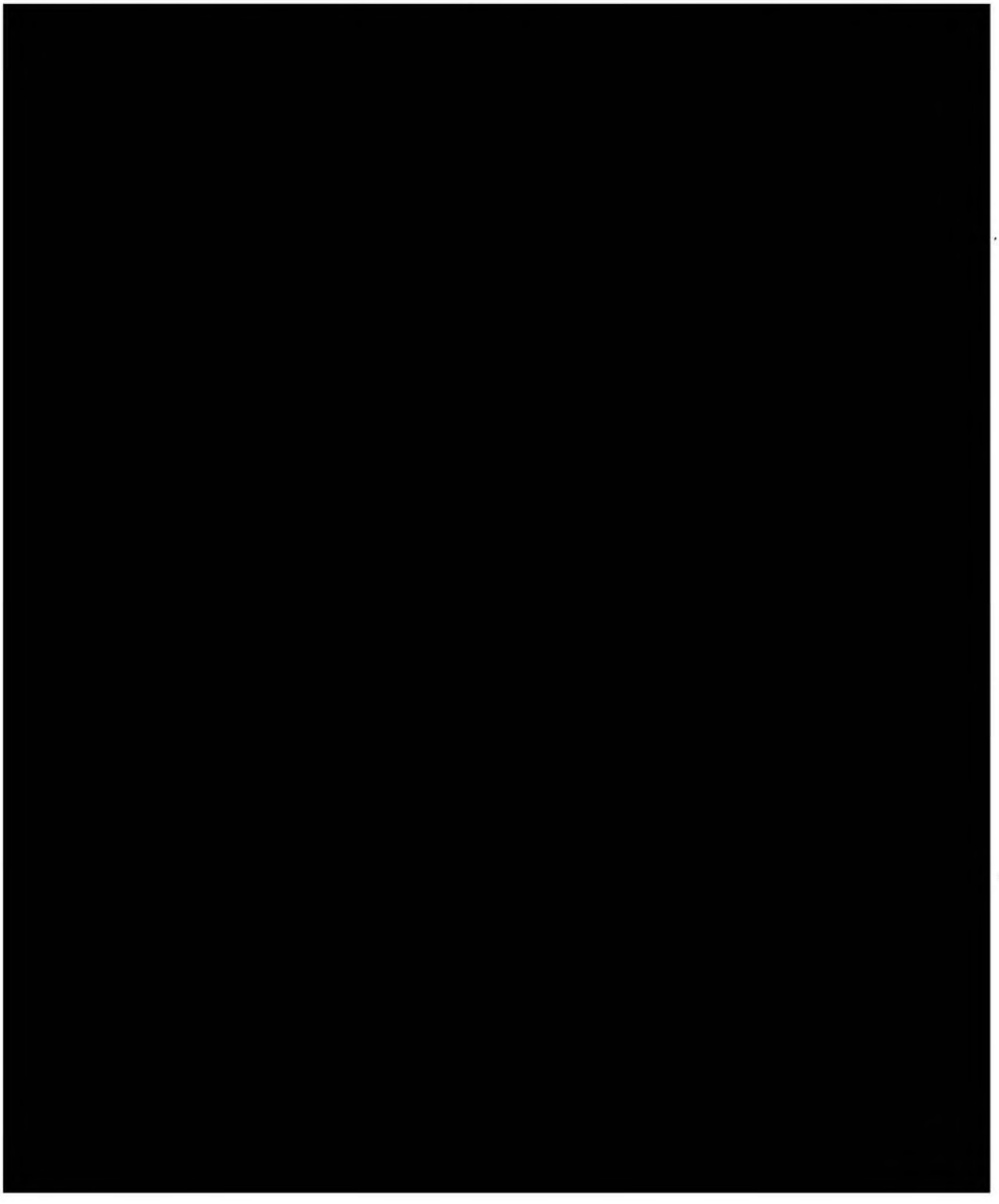
k) [redacted]

Invite feedback on the interview, and ask if there is anything else which the individual may wish to discuss.

APPENDIX "B"

1. REPORTS CONTAINING NO TRACES

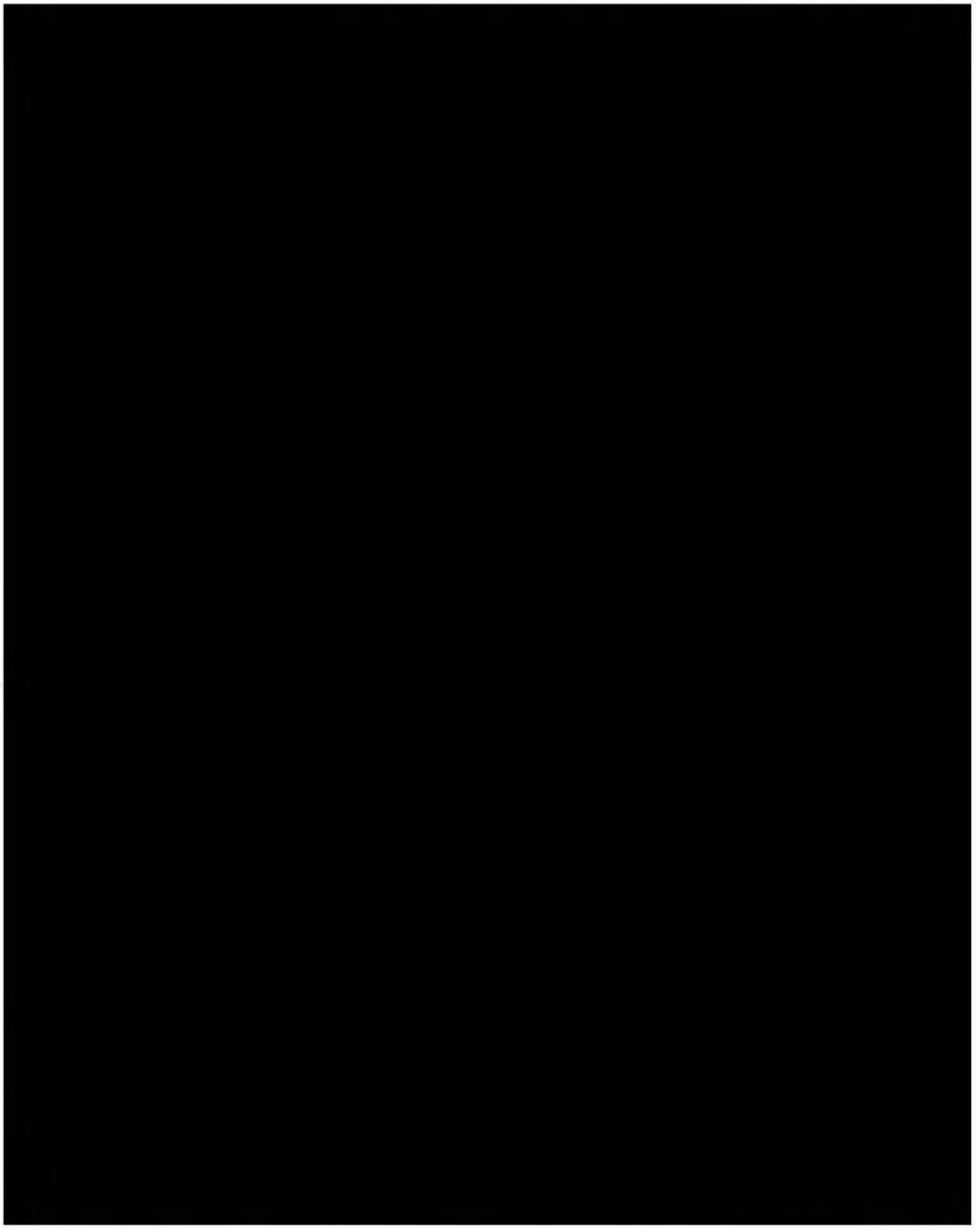


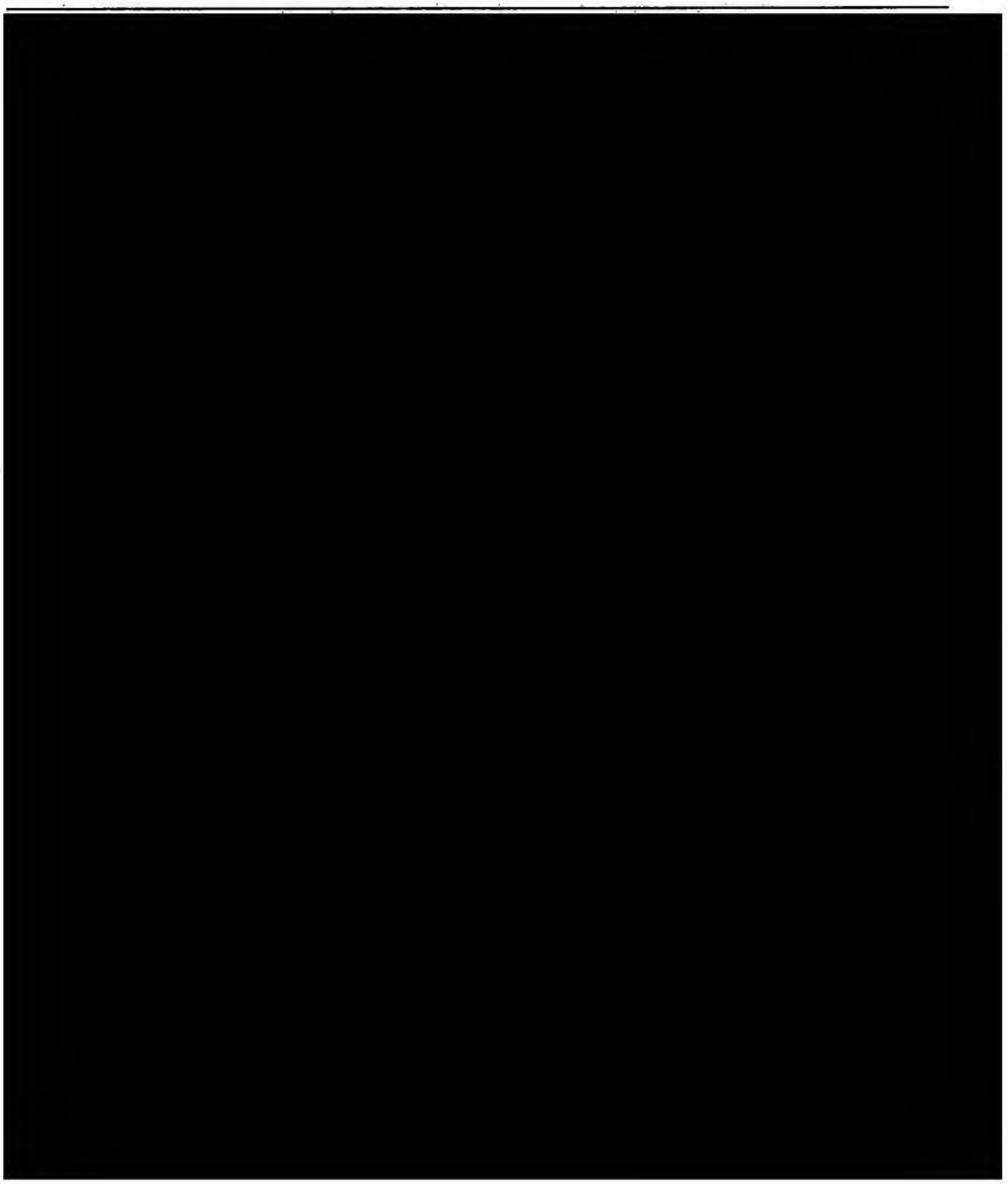


[redacted]

2. REPORTS CONTAINING TRACES:

[redacted]





3. [redacted]

4. CSIS APPLICANTS

Investigators must submit two reports when dealing with CSIS applicants. One covers the security investigation and is addressed to Security Screening; the second separate report covers suitability issues, and is sent to Personnel Services.

When submitting these reports, use the following introductions:

Security clearance report submitted to Security Screening

This report is submitted at the request of the Director General, Security Screening, CSIS, to provide a security assessment, in relation to the individual's loyalty to Canada and insofar as it relates thereto his/her reliability. Its use is intended to assist the Director General of Internal Security, CSIS, in the determination of whether to grant or deny a security clearance.

Suitability report submitted to Personnel Services

This report is submitted at the request of the Director General, Personnel Services, CSIS to provide a suitability assessment of the individual's candidacy for employment with CSIS. Its use is intended to assist in the determination of whether or not the individual would make a suitable employee for CSIS.

The following are the "suitability factors" to be considered by the investigator. They encompass a subject's qualifications and character assessment:

1) VERIFICATION OF QUALIFICATIONS:

Education: To ensure that the candidate possesses the academic qualifications stated on screening form and/or resumé, the most recent school or that institution where subject's highest degree was awarded should be contacted. Not all subject's diplomas, degrees need be verified; however, if the investigator is not satisfied with information received from sources regarding

subject's educational qualifications, other academic institutes should be contacted.

Employment: To evaluate experience in relation to the requirements of the position, where possible, interview past and present employers* and co-workers to solicit opinions regarding:

- subject's attitude towards work, authority and fellow workers;
- subject's performance and suitability, i.e., absenteeism, tardiness, knowledge and potential, work habits;
- personal deportment/behaviour;
- level (s) attained;
- reason for termination;
- subject's rehireability.

*Note: If candidate has indicated present employment may be jeopardized if present employer is contacted:

- try to obtain results using alternate methods;
- contact CSIS Personnel Services to approach candidate for assistance.

2) CHARACTER ASSESSMENT:

Assessment of subject's suitability to work for the Service in terms of behaviour - in the workplace and socially. There is obviously some overlap between suitability for the job, and some aspects affecting reliability as it relates to loyalty. The emphasis in the suitability report is on the subject's behaviour in the workplace: work ethic; temperament; attitude; sociability; maturity; etc. Tactful enquiries by the investigator of those familiar with the candidate will reveal information of this sort.

Additional information should be pursued:

[redacted]

[redacted]

Oftentimes a close friend may not wish to reveal information on the subject which might jeopardize the latter's employment opportunities. However, if the investigator takes the time to explain the rationale behind the screening program and the fact that by not being totally honest, the friend will not be doing the subject a favour because:

1) the subject may be placed in a position for which he is not qualified;

2) after occupying the position, subject's lack of qualifications may cause him to fail in the position and be eventually terminated;

3) if adverse reliability features exist, they may surface again after subject's engagement, thus leading to possible termination;

4) because the subject is to be entrusted with secure assets protected in the national interest, the source may indirectly harm national security by failing to be honest about the subject's loyalty and reliability.

5) the source can be assured complete anonymity by the investigator. The subject has knowingly consented to allowing CSIS to interview friends, neighbours, employers, etc., but the subject will not know the identity of the people spoken to. Source identification is protected under the Access to Information and Privacy Acts. It is also preferable that the source not tell the subject the interview took place.

Therefore, most "real" friends should be mature enough to provide valid assessments when the program is properly understood.

Character References: References named by the candidate should know the subject well enough to provide a worthwhile assessment, e.g., any undesirable traits candidate possesses. Ideally, references should be over 18 years of age and not related to the subject. The opinions of character references are important.

The Regions are reminded that CSIS candidates are afforded priority tasking, and that it is incumbent upon all investigators working on such cases to pay equal attention at preparing both the security and the suitability reports for HQ.

5. REPORTS FOR LEVEL III UPDATES - No trace information uncovered

[redacted]

6. REPORTS FOR LEVEL III UPDATES - Trace information uncovered

[redacted]

SECTION B) IMMIGRATION AND CITIZENSHIP SCREENING CAN BE FOUND ON FILE "SSPM IMM ENGLISH"

C) CONCLUSION - REGIONAL ACCOUNTABILITY

Field reports are the base on which accountability rests for all significant security screening investigations. Accountability must exist in any government program, particularly one that impacts so much on the privacy and lives of Canadians, the admissibility of prospective new immigrants and, in some cases, the eventual granting of citizenship.

During a screening investigation under the GSP, the investigator should be focused on providing a security assessment of a subject, in total. This is why screening personnel should be just as meticulous in documenting positive features of character, as in detailing, resolving and confronting, if necessary, any negative aspects that appear. In the interests of reporting and ensuring a timely reply to our clients, only full details on adverse cases need be documented all the way up the "reporting chain" to HQ personnel.

As referred to earlier in this guide, the security screening program is the most visible face of CSIS and therefore its biggest area of public relations. This puts the onus on the investigator and analyst alike to provide the best possible service to our clients (includes file subjects as well as requesting Departments and contracting companies). During any part of the security screening investigation, any complaint regarding processing delays, line of questioning, validity of the program, etc., should be documented in the report for the attention of Regional and HQ Management. The investigator should also advise the complainant, where appropriate, of further redress, e.g., telephone number of supervisor or the formal appeal process Assessment of subject:through the Security Intelligence Review Committee (SIRC).

The quality control program that operates within the security screening program reflects a firm commitment on the part of the Security Screening Branch to improve the quality of our investigations and ensure that the security assessments provided to our government clients are valid. In that vein, files are selected at random for monthly quality control purposes. It is incumbent upon the investigator to conduct his investigations professionally, to report his findings accurately and in accordance with the Service's policy. With this shared commitment on behalf of all the players within the program, both Regional and HQ, we will continue to provide the high level of security screening service that has become recognized as a valuable and integral role for CSIS within the Canadian security community.