Canada Border Services Agency

Immigration Control (IC) Manual – Chapter 1

Security Screening Process Manual

Document Changes and Updates Tracking – August 30, 2016

Updates:

August 30, 2016

The Immigration Control (IC) Manual Chapter 1 - Security Screening of Permanent Residence Applications and the Immigration Control (IC) Manual – Chapter 2 – Security Screening of Temporary Residence Applications were consolidated into an Immigration Control Process Manual and an Immigration Control Indicator Manual.

This manual chapter, the **Immigration Control (IC) Manual – Chapter 1 Security Screening Process Manual** provides procedural guidance on **how** to refer applications for temporary and permanent residence to the Canada Border Services Agency (CBSA) and screening partners for security screening pursuant to sections 34, 35 and/or 37 of the *Immigration and Refugee Protection Act* (IRPA).

The **Immigration Control (IC) Manual – Chapter 2 Security Screening Indicator Manual** provides guidance on **when** to refer applications to the CBSA and screening partners for security screening and direction on the use of the screening indicators, lists of mandatory screening countries, indicators and general screening indicators.

Table of Contents

1. What is this chapter about? 5
2. Program objectives 5
3. The Act and Regulations 5
3.1 Supporting documents 9
3.2 Official languages 9
4. Instruments and Delegations 9
5. Classification of information 10
5.1 Classification of information received from screening partners 10
5.2 Information at the Protected B Level 11
5.3 Information at the Secret Level 11
6. Disclosure of information 11
6.1 Information regarding the screening process 11
6.2 Releasing Case Information to Applicants 12
6.3 Releasing Case Information obtained from Partners 12
6.4 Access to Information and Privacy Requests 12
7. The security screening process 13
7.1 What is security screening? 13
7.2 What is a security screening request? 13
7.3 Screening tools 13
8. Security screening: roles and responsibilities 14
8.1 Mandate: Immigration, Refugees and Citizenship Canada 14
8.2 Mandate: National Security Screening Division (NSSD) at the CBSA 14
8.3 Mandate: Canadian Security Intelligence Service (CSIS) 14
9. Screening Guidelines - General 15
9.1 Decision makers must explore all grounds of inadmissibility 15
9.2 Mandatory screening referrals 15
9.3 Discretionary screening referrals 16
9.4 Minor children 17
10. Screening Guidelines for Temporary Resident Applications 18
10.1 Security Screening Requests 18
10.2 Where to send security screening requests during a GCMS outage 19
10.3 Sending security screening requests to security screening partners 19
10.4 Urgent Screening Requests/VIP Cases via GCMS 19
10.5 Very Important Persons (VIP) – Priority Security Screening Procedures 20
10.6 Security screening request (VIT) after a TRV has been issued 23
10.7 Service standards for screening temporary resident applications 23
10.8 HOLD on cases 24
10.9 NIL response 25
10.10 Interim Procedures for Cases that must be Expedited where the 10 Working Day Security Screening Service Standard has been Exceeded 26
10.11 Validity of screening results – temporary resident applications 26
10.12 Additional Information 26
10.13 Multi-Entry Visas (MEV) versus Single-Entry Visas 27
11. Screening Guidelines for Permanent Resident Applications 27
11.1 Records check versus comprehensive check 28
11.2 Sending security screening requests from visa offices and the case processing centre – Ottawa 27
11.3 Sending applications for permanent residence for security screening from inland offices 30
11.4 Service delivery standards for screening permanent resident applications 30
11.5 Validity of screening results (permanent resident applications) 30
12. Screening Guidelines for front end security screening of refugee protection claimants 31
12.1 Front End Security Screening Background 31

12.2 Preparing security screening requests 31
12.3 Inland Claims (IRCC) 31
12.4 POE Claims (CBSA referrals) 31
12.5 Service Standards 31
12.6 Ineligible Claimants 31
12.7 Identity verification for claimants who are in detention 32
12.8 Abandoned Claims 32
12.9 Screening results 32
13. Global Case Management System (GCMS) 32
14. Security screening interviews to obtain additional information (for all streams) 33
14.1 Consulting and inviting partners to interviews 33
15. Screening results returned to IRCC (for all streams) 33
15.1 Inadmissibility recommendations (CBSA) 33
16. Admissibility determination (IRCC) 34
17. Contrary outcomes 35
17.1 Definition: 35
17.2 Contrary outcome scenarios 35
17.3 Instructions for Processing Contrary Outcome cases at visa offices and at Case Processing Centre-Ottawa 36
17.4 The CBSA's role 38
17.5 Communicating the decision 38
17.6 Additional References 39
18. Refusals under section(s) 34, 35 and/or 37 of IRPA 40
18.1. High profile, contentious and sensitive cases 40
19. Responses to a refusal 41
20. Lookouts/Alerts 41
21. Remedies 41
21.1. Remedies to facilitate temporary residence 41
21.2. Remedy to facilitate permanent residence 42
Applications for Ministerial Relief (MR) 42
22. Other related processes 42
22.1. The Foreign Missions and International Organizations Act 42
22.2. FMIOA Security Screening and Advising NHQ 42
22.3. Port of entry screening 43
23. Seizure of documents 44
24. Inland security screening 44
24.1 Extension or change of status 44
24.2 Work and study permits issued in Canada and overseas 44
Appendix A - Protected and Classified Information 45
Appendix B – Screening Tools 49
Appendix C - Overview of the security screening process 56
Appendix D: Sending Security Screening Requests (VITs) for TR applications by email in the event of GCMS outage 57
Appendix E: Basic areas to be explored during the interview 60
Appendix F – Who to contact at HQ 68

1. What is this chapter about?

This manual chapter provides procedural guidance and direction to officers on how to send security screening requests to the Canada Border Services Agency (CBSA) and screening partners for temporary and permanent resident applications and claims for refugee protection. More specifically, this manual chapter provides functional direction and guidance to:

- Officers who are responsible for making decisions on the admissibility of foreign nationals pursuant to section(s) 34, 35 and/or 37 of the *Immigration and Refugee Protection Act* (IRPA).
- Officers responsible for making decisions on the admissibility of foreign nationals who are applying for an extension or a change of their valid temporary resident status in Canada, pursuant to section(s) 34, 35 and/or 37 of IRPA.
  - A34 - Security (espionage, subversion, terrorism)
  - A35 - War crimes, crimes against humanity and genocide
  - A37 - Organized or transnational criminality

1. Program objectives

The objectives of Canadian immigration legislation, relative to the security provisions, are:

- to protect the health and safety of Canadians and to maintain the security of Canadian society;
- to promote international justice and security by fostering respect for human rights and by denying access to Canadian territory to persons who are serious criminals or security risks.

2. The Act and Regulations

Officers responsible for assessing admissibility should be familiar with the legislative and regulatory authorities contained within IRPA and its accompanying regulations. The following authorities relate to assessing admissibility with respect to section(s) 34, 35 and/or 37 of IRPA.

Reference to Act or Regulations	Provision
A11.1	Requirement of certain foreign nationals who make an application for a temporary resident visa, study permit or work permit to submit biometric information.
A11(1)	A foreign national must, before entering Canada, apply for a visa or for any other document required by the regulations. The visa or document may be issued if, following an examination, the officer is satisfied that the foreign national is not inadmissible and meets the requirements of this Act.

Reference to Act or Regulations	Provision
R12.1(1)	Countries and territories whose nationals are required to provide biometric information.
R.12.1(2)	Exemptions from the requirement to provide biometric information.
A15(1)	An officer is authorized to proceed with an examination where a person makes an application to the officer in accordance with this Act.
A16(1)	A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires.
A16(1.1)	A person who makes an application must, on request of an officer, appear for an examination.
A16(2.1)	A foreign national who makes an application must, on request of an officer, appear for an interview for the purpose of an investigation conducted by the Canadian Security Intelligence Service under section 15 of the *Canadian Security Intelligence Service Act* for the purpose of providing advice or information to the Minister under section 14 of that Act and must answer truthfully all questions put to them during the interview.
A18(1)	Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada.
A20(1)(b)	Every foreign national, other than a foreign national referred to in section 19, who seeks to enter or remain in Canada must establish, to become a temporary resident, that they hold the visa or other document required under the regulations and will leave Canada by the end of the period authorized for their stay.
A22(1)	A foreign national becomes a temporary resident if an officer is satisfied that the foreign national has applied for that status, has met the obligations set out in paragraph 20(1)(b) and is not inadmissible.
A24(1)	A foreign national who, in the opinion of an officer, is inadmissible or does not meet the requirements of the Act becomes a temporary resident if an officer is of the opinion that it is justified in the circumstances and issues a temporary resident permit, which may be cancelled at any time.

Reference to Act or Regulations	Provision
A24(2)	A foreign national referred to in subsection (1) to whom an officer issues a temporary resident permit outside Canada does not become a temporary resident until they have been examined upon arrival in Canada.
A24(3)	In applying subsection (1), the officer shall act in accordance with any instructions that the Minister may make.
A33	The facts that constitute inadmissibility under sections 34 to 37 include facts arising from omissions and, unless otherwise provided, include facts for which they are reasonable grounds to believe that they have occurred, are occurring or may occur.
A34(1)	A permanent resident or a foreign national is inadmissible on security grounds for:
A34(1)(a)	• engaging in an act of espionage that is against Canada or that is contrary to Canada's interests
A34(1)(b)	• engaging in or instigating the subversion by force of any government;
A34(1)(b.1)	• engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada;
A34(1)(c)	• engaging in terrorism;
A34(1)(d)	• being a danger to the security of Canada;
A34(1)(e)	• engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or
A34(1)(f)	• being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c).
A35(1)	A permanent resident or a foreign national is inadmissible on grounds of violating human or international rights for
A35(1)(a)	• committing an act outside Canada that constitutes an offence referred to in sections 4 to 7 of the *Crimes Against Humanity and War Crimes Act*;
A35(1)(b)	• being a prescribed senior official in the service of a government that, in the opinion of the Minister, engages or has

Reference to Act or Regulations	Provision
	engaged in terrorism, systematic or gross human rights violations, or genocide, a war crime or a crime against humanity within the meaning of subsections 6(3) to (5) of the *Crimes Against Humanity and War Crimes Act*; or
R16	For the purposes of paragraph A35(1)(b) of the Act, a prescribed senior official in the service of a government is a person who, by virtue of the position they hold or held, is or was able to exert significant influence on the exercise of government policy or is or was able to benefit from their position, and includes:
R16(a)	• heads of state or government;
R16(b)	• members of the cabinet or governing council;
R16(c)	• senior advisors to persons described in paragraph (a) or (b);
R16(d)	• senior members of the public service;
R16(e)	• senior members of the military and of the intelligence and internal security services;
R16(f)	• ambassadors and senior diplomatic officials; and
R16(g)	• members of the judiciary.
A35(1)(c)	• being a person, other than a permanent resident, whose entry into or stay in Canada is restricted pursuant to a decision, resolution or measure of an international organization of states or association of states, of which Canada is a member, that imposes sanctions on a country against which Canada has imposed or has agreed to impose sanctions in concert with that organization or association.
A37(1)	A permanent resident or a foreign national is inadmissible on grounds of organized criminality for
A37(1)(a)	• being a member of an organization that is believed on reasonable grounds to be or to have been engaged in activity that is part of a pattern of criminal activity planned and organized by a number of persons acting in concert in furtherance of the commission of an offence that is punishable under an Act of Parliament by way of indictment, or in furtherance of the commission of an offence outside Canada that, if committed in Canada, would constitute such an offence or engaging in activity that is part of such a pattern; or

Reference to Act or Regulations	Provision
A37(1)(b)	• engaging, in the context of transnational crime, in activities such as people smuggling, trafficking in persons or money laundering.
83.05 (1) *Criminal Code of Canada*	The Governor in Council may, by regulation, establish a list on which the Governor in Council may place an entity if, on the recommendation of the Minister of Public Safety and Emergency Preparedness, the Governor in Council is satisfied that there are reasonable grounds to believe that
83.05 (1)(a) *Criminal Code of Canada*	• the entity has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or,
83.05 (1)(b) *Criminal Code of Canada*	• the entity is knowingly acting on behalf of, at the discretion of or in association with an entity referred to in paragraph (a).

3.1 Supporting documents

In accordance with section 16(1) of IRPA, persons who make an application for temporary or permanent residence must produce all relevant evidence and documents that an officer reasonably requires to assess admissibility including, but not limited to letters of invitation, financial statements, itineraries, etc.

To conduct meaningful security screening, the CBSA and screening partners require the following documents at a minimum:

- Application form;
- Applicable Schedule; and,
- Supplementary information that may assist screening partners.

3.2 Official languages

Application forms **must** be completed in either official language of Canada (French or English).

All supporting documentation must be in English or French; or if supporting documentation is not in English or French, it **must be accompanied** by:

- the English or French translation; and
- an affidavit from the person who completed the translation; and
- a certified photocopy of the original document.

4. Instruments and delegations

Refer to the Immigration Legislation Manual (IL3) for specific delegations of authority for sections 34, 35 and 37 of IRPA. This manual refers to the Designation of Officers and Delegation of Authority document, which sets out the persons or class of persons designated by the Minister as officers to carry out any purposes of the Act and specifies the powers and duties of the officers so designated.

Policy responsibility with respect to sections 34, 35 and 37 of IRPA, is with the CBSA. Immigration, Refugees and Citizenship Canada (IRCC) is responsible for service delivery as follows:

Area	Service Delivery
Overseas	IRCC
Port of Entry	CBSA
In Canada	IRCC and the CBSA

5. Classification of information

This manual chapter is classified 'Protected B' because it contains information about the security screening process, which if released could compromise government strategy on preventing individuals who pose a risk from coming to Canada. All parties involved in the security screening process must ensure that this information is accessible only to individuals with the appropriate security clearance who are involved in the security screening process.

5.1 Classification of information received from screening partners

As provided for in policy and law and in an effort to protect and foster relationships with our screening partners, it is imperative that all information be afforded the appropriate protection according to its classification. This includes electronic transmissions, the use of remarks in systems of record such as the Global Case Management System (GCMS), storage and transportation of documents as well as the release of information.

In accordance with the Policy on Government Security the classification of information is at the discretion of the originating agency and must not be re-classified to a lower level at any time. Officers must ensure that they apply appropriate safeguards to partner information based on security classification as indicated.

5.2 Information at the Protected B level

Much of the information gathered by and transmitted between the CBSA and IRCC on immigration applications, including security screening requests, is classified at the "Protected B" level. Security screening requests and admissibility recommendations that are classified at the Protected B level can be uploaded and transmitted

[redacted] as per the CBSA's *Information Classification Guide* (Appendix A).

5.3 Information at the Secret level

Information provided to IRCC and the CBSA by partner agencies to assist in making a recommendation and/or decision on admissibility is often classified at the "Secret" level or above. This information must be transmitted

[redacted] as per CBSA's *Information Classification Guide* (Appendix A). This information should only be accessible to officers with the appropriate security clearance and the 'need to know'.

6. Disclosure of information

In accordance with the *Policy on Government Security*, the CBSA and IRCC must protect the confidentiality, integrity and availability of the information and assets in its care.

6.1 Information regarding the screening process

Officers involved in the screening process are not to discuss specific elements of the screening process with clients, their representatives, the public or the media. **To this end, officers shall not:**

- **Release or record in GCMS or e-mail, the names of screening partners;**
- **Release or record in GCMS or e-mail the names of any officers from IRCC, CBSA or any other agency involved in the screening process;**
- **Refer clients or their representative to IRCC, CBSA or other agency**

If questioned about the screening process by applicants and/or their representative (i.e. designated individuals, authorized representatives), officers may indicate that all foreign nationals, including temporary residents, are subject to background verifications and that cases cannot be finalized until all verifications are complete. Officers may also indicate that verifications may include police and other types of background checks.

Note: If required, officers may include notes in GCMS and/or in e-mails indicating that "partners are being consulted", without specifying the name of the partner agency or the nature of the concerns being investigated.

6.2 Releasing case information to applicants

Case specific, **unclassified** information may only be released by an IRCC officer to applicants or their representative once the client has been clearly identified and has made a formal request, or once the client's representative has provided the required authorization from the client.

Classified, including information that is classified by CSIS as I , or sensitive information must never be released to applicants or their representatives. Such disclosure has the potential to compromise sources and irrevocably affect the relationships and interests of the Government of Canada. This is true in particular (but not exclusively) for information provided to officers by foreign agencies, directly or through partners.

Officers should consult with screening partners to determine what information can be disclosed to the applicant. For additional guidance, refer to section 17 of this manual (Concurrent outcomes).

Note: Information caveated as is provided to IRCC officers as lead information RRC officers may reference this information as having been previously provided to Canadian government officials by the applicant.

Information provided to IRCC and the CBSA by partner agencies to assist in making a recommendation and/or decision on admissibility is often classified at the "Secret" level. This information must be transmitted Managers must ensure that this information is only accessible to officers with the appropriate security clearance and a "need to know".

6.3 Releasing case information obtained from partners

Information provided by screening partners is normally provided as an investigative tool to assist IRCC decision-makers in arriving at well-informed decisions.

Unclassified and protected B information may be released. However, when information marked as unclassified is based on classified information, including information classified by CSIS as officers must take care to ensure the release of the unclassified information does not jeopardize or identify the nature of the classified information.

Classified information is not to be released to applicants, counsel or to the general public without written consent from the applicable partner agency.

Release of classified information provided by the National Security Screening Division (NSSD) requires written permission from the NSSD.

6.4 Access to information and privacy requests

Access to information or privacy (ATIP) requests made under the *Access to Information Act* (ATIA) or *Privacy Act* (PA) will be directed to the Access to Information and Privacy Coordinators from within the CBSA or IRCC, depending on the nature of the request.

The area responsible for responding to a particular request shall search for and provide all related records. In addition, the responsible area will include recommendations with respect

to the information that should not be released based on provisions contained in the ATIA and the PA. A rationale to support recommendations for non-disclosure must be provided.

Officers are strongly encouraged to contact the NSSD and CSIS, should they require assistance in examining classified documents and ensuring appropriate exemptions are applied prior to releasing the information.

The NSSD and screening partners must be consulted prior to the release of any information that they provided.

7. The security screening process

7.1 What is security screening?

Section 11(1) of IRPA stipulates that before entering Canada a foreign national must apply to an officer for a visa or any other document required by the regulations. The visa or document may be issued if, following an examination, the officer is satisfied that the foreign national is not inadmissible and meets the requirements of IRPA. Security Screening is conducted to support decision-makers in making well-informed admissibility determinations.

Officers who have reason to believe that an applicant may be inadmissible pursuant to section(s) 34, 35 and/or 37 of IRPA, but need additional information to make a determination, should send a request for security screening to the NSSD and screening partners as applicable.

The importance of the security screening process cannot be overstated. Officers are mandated to protect the safety and security of Canadians and to prevent Canada from becoming a haven for those fleeing justice elsewhere, who pose a security threat to Canada and whose entry would be detrimental to Canada's national interest.

The security screening process includes the collection of information from a variety of sources, including open source research and classified systems. Once collated, the information is analyzed to determine if it is sufficient to support an inadmissibility recommendation pursuant to section(s) 34, 35 and/or 37 of IRPA.

7.2 What is a security screening request?

- A security screening request is a message transmitted to the NSSD and screening partners to request in-depth screening of a person's background as per the instructions in this manual chapter.
- In the overseas context, Locally Engaged Staff (LES) can be tasked with preparing and transmitting security screening requests as long as classified or sensitive material is not included. When classified or sensitive material is involved, only officers with the appropriate security clearance can have access to or transmit the security screening request.
- Classified information should only be sent by secure means as appropriate according to its classification level, not through GCMS.

7.3 Tools available to IRCC officers

There are a number of classified and open source tools available to assist IRCC officers in making a determination regarding inadmissibility pursuant to section(s) 34, 35 and/or 37 of IRPA. Tools include GCMS, the updated Immigration Control Indicator manual (IC 2), the CBSA intranet and the Internet (for additonal information on screening tools, refer to Appendix B of this manual chapter).

8. Security screening: roles and responsibilities

The roles and responsibilities of the departments and agencies involved in the security screening process are as follows:

8.1 Mandate: Immigration, Refugees and Citizenship Canada

Immigration, Refugees and Citizenship Canada (IRCC) officers review applications for temporary and permanent residence to ensure applications are complete and to make admissibility and eligibility decisions.

When warranted, officers refer applications in accordance with instructions provided in this manual to the CBSA and screening partners for security screening. Taking into consideration all available information, officers decide whether or not to issue a temporary or permanent resident visa, as the case may be.

8.2 Mandate: National Security Screening Division at the CBSA

The National Security Screening Division (NSSD) screens applicants for temporary and permanent residence and refugee protection claimants for possible involvement in activities that would render applicants inadmissible to Canada pursuant to section(s) 34, 35 and/or 37 of IRPA.

The NSSD conducts research using open source and classified information. Based on a thorough analysis of all available information, the NSSD develops inadmissibility recommendations that are provided to IRCC decision makers to support their determination on admissibility.

For questions related to security screening referrals, officers may contact the NSSD via

8.3 Mandate: Canadian Security Intelligence Service (CSIS)

CSIS provides advice on threats to the security of Canada in accordance with Section 14 of the CSIS Act to the CBSA and IRCC to assist in the exercise of duties and functions in accordance with IRPA, particularly as it relates to current national security concerns pursuant to paragraphs A34(1)(a), (c), (d) and (f) of IRPA.

Section 2 of the CSIS Act defines threats to the security of Canada as follows:

> (*a*) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(*b*) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(*c*) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).

The decision to issue or refuse a temporary or permanent resident visa rests with IRCC officers.

Note: CSIS focuses on present and potential future threats to the security of Canada only and does not provide advice with respect to an applicant's admissibility to Canada.

Note: Notwithstanding a final determination by IRCC decision makers to issue a temporary or permanent resident visa, CBSA Border Services Officers (BSO) must be satisfied that an individual is not inadmissible before granting entry into Canada. [Status and authorization to enter: Subsection 21(1) of IRPA for permanent residents and subsection 22(1) for temporary residents].

9. Screening guidelines - general

9.1 Decision makers must explore all grounds of inadmissibility

- When reviewing applications, IRCC officers should consider all of the inadmissibility provisions under IRPA.
- Officers should concurrently evaluate applications in relation to inadmissibility with respect to section 36 (serious criminality and criminality), section 38 (health grounds), section 39 (financial reasons), section 40 (misrepresentation), section 41 (non-compliance with IRPA) and section 42 (inadmissible family member).

Note: If inadmissibility pursuant to section 36, 38, 39, 40, 41 and/or 42 is determined,

Note: If a security screening referral has already been sent, officers should cancel the request.

9.2 Mandatory screening referrals

For applicants who are not inadmissible pursuant to sections 36, 38, 39, 40, 41 and/or 42 of IRPA,

Note: pursuant to sections 34, 35 and/or 37 of IRPA can be determined based on available information, [redacted] Referral for security screening is not required.

9.3 Discretionary screening referrals

Note: pursuant to sections 34, 35 and/or 37 of IRPA can be determined

Applications that meet any of the criteria below may be referred for security screening at the officer's discretion:

Errors and incomplete applications slow down the screening process. IRCC officers should ensure that the referral includes all required information and available details on adverse information, when sending a security screening referral. This will assist screening partners in narrowing their research and allows the NSSD to provide IRCC officers with a comprehensive recommendation in a timely manner.

Note: Notwithstanding a final determination by an IRCC decision maker to issue a temporary or permanent resident visa, CBSA Border Services Officers (BSO) must be satisfied that an individual is not inadmissible before granting entry to Canada. [Status and authorization to enter: Subsection 21(1) of IRPA for permanent residents and subsection 22(1) for temporary residents].

9.4 Minor children

Children under the age of 18 generally do not require security screening. However, if special circumstances are such that screening is required, applications from minor children may be referred for security screening. For example,

the application should be refered for security screening.

10. Screening guidelines for temporary resident applications

For a visual representation of the security screening process, refer to Appendix C.

10.1 Security screening requests

When it has been determined that an applicant requires security screening because the applicant meets mandatory or discretionary screening indicators (refer to IC Indicator Manual) ((section 4 of the IC Indicator Manual), or the officer suspects that the applicant may be inadmissible pursuant to section(s) 34, 35 and/or 37 of IPRA, a security screening request [previously known as Visitor Information Transmission (VIT)] is sent to the NSSD and screening partners via GCMS to request screening of an applicant's background.

10.2 Where to send security screening requests during a GCMS outage

In the event of a GCMS failure, security screening requests may be sent by e-mail using the VIT template in Appendix D. All of the information required in the VIT template or GCMS fields must be provided and transmitted to the NSSD via following the instructions outlined in Appendix D.

Note: This procedure is reserved for emergency situations only.

- Depending on the type of referral, security screening requests that are sent via email must be referred according to the section of IRPA for which screening is requested. When sending a security screening request via GCMS, officers indicate for which section of the Act screening is requested: VIT 34, VIT 35, and/or VIT 37, as applicable. The system requires that officers include case details prior to sending the security screening request.

10.3 Sending security screening requests to security screening partners

Security screening requests that are sent via GCMS go to the NSSD and security screening partners as follows:

Section of IRPA	Security Screening GCMS Values	Case goes to
34	VIT 34	CBSA, CSIS
35	VIT 35	CBSA
37	VIT 37	CBSA

Note: To make GCMS case notes and other relevant documents (e.g. police tables, military information tables, etc.) available to screening partners, the documents should be uploaded to GCMS under the relevant screening sub-activities tab, under the 'attachment' tab so that partners have access to this information in GCMS.

Note: For information on how to attach information to the security screening request, refer to GCMS online help.

10.4 High priority screening requests

Note: Requests for expedited processing create disproportionate demands on the screening capabilities of the NSSD and screening partners, which can quickly become unmanageable and threaten the integrity of the entire screening system. In addition, such requests perpetuate the erroneous perception that all processing could be completed well within the standard waiting period, resulting in increased pressure to expedite as the norm. **Consequently, requests for expedited processing will only be accommodated in the most compelling circumstances when a clearly articulated rationale, citing national interest or humanitarian and compassionate grounds, is provided.**

10.4.1 Urgent screening requests – priority security screening procedures

Type of security screening request (VIT)	Email information
Urgent screening requests	**To** **Subject:** URGENT Request: UCI <12345678> **Body of email:**

	Name: <Frank RUSHMORE> DOB: <YYYY/MM/DD> UCI: <12345678> Requested date: <YYYY/MM/DD> **Note:** The requested date must be a CBSA Head Quarters (HQ) working day, and IRCC's Case Management Branch (CMB) must be copied via on all urgent requests, The NSSD will facilitate communication between the visa office and screening partners for all urgent processing cases.
Note: Visa offices should send an advance email notifying the NSSD via of upcoming security screening requests for Delegations.	

10.4.2 Very Important Person (VIP) – priority security screening procedures

- Individuals must fall into a VIP category, as outlined on the list below in order to be processed as a VIP.
- Officers who receive TRV applications that fall into a VIP category and require security screening should continue to refer these applications to the NSSD for screening via GCMS.
- For screening requests that fall within the VIP category, officers should select screening referral type 'priority', as opposed to 'normal'.
- The VIP process applies to the following categories of people:
  1. Heads and deputy heads of state
  2. Chief justices
  3. Parliamentary and senate speakers
  4. Ministers and deputy ministers; secretaries of state
  5. Parliamentary secretaries
  6. Lieutenant governors
  7. Provincial and territorial leaders and ministers
  8. Federal parliamentarians
  9. Assistant Deputy Minister-level senior federal, provincial and territorial officials

10. Individuals covered by an Order in Council (OIC) under the *Foreign Missions and International Organizations Act* (FMIOA)

11. In exceptional circumstances, other individuals identified by the Immigration Program Manager (IPM) who may be considered a VIP (senior business people equivalent to the government positions mentioned above, cases that are considered to be within the national interest or cases that may risk creating a significant bilateral irritant).

For category 11 clients, the IPM, as per the Instrument of Designations and Delegations, must approve the request for expedited processing and must be copied on the message sent to the CBSA.

Note: The VIP process applies only to principal applicants, and not to individuals accompanying the VIP. If urgent processing is required for accompanying individuals or past occupants of these positions, then national interest urgent processing should be requested.

10.4.3 Humanitarian and compassionate grounds

Officers and IPMs should use their discretion in determining whether or not an application requires high priority security screening for humanitarian and compassionate (H&C) grounds. Prior to issuing a request for high priority screening, officers should ensure that travel dates can not be facilitated through regular processing.

Examples of cases that **qualify** for high priority security screening for H&C grounds include, but are not limited to:

- Travel to attend a funeral or a gravely ill immediate family member
- Travel for urgent medical reasons

Examples of H&C grounds cases that **do not qualify** for high priority security screening include, but are not limited to:

- A client who needs to travel in order to be able to attend the first day of classes or to attend a conference,
- A client who has purchased a plane ticket in advance and the purchase is not refundable.

The IPM, as per the Instrument of Designations and Delegations, must approve the request for expedited processing on the basis of H&C grounds and must be copied on the message sent to the CBSA.

10.4.4 Procedures for sending high priority requests

1) Determine if the application meets the criteria for high priority screening and seek IPM approval.

2) Ensure all relevant information is available in the GCMS file. Should partners require further information, the CBSA will contact the visa office, which may impact service standards.

3) Using the appropriate email template below, articulate the rationale for the high priority screening request and copy and paste this information into the "notes" field, by creating a new note. Once the note is saved, select the "restricted" box beside the note.

4) Send the security screening request via GCMS as follows:

- within GCMS, create, but do not submit the screening request;
- in the sub-activity, click on the ' to see the whole activity;
- set priority to 'High'; and
- set status to 'Submit'

5) Submit the rationale for the screening request to the CBSA by email using the template below.

Note: If the applicant also meets the criteria for a high-profile, complex, sensitive or contentious case, please ensure you follow the relevant Program Delivery Instructions and send a **separate** email. **Please do not copy the nhq-nat-high-profile distribution list when sending high priority referrals to the CBSA.**

10.5 Email template – rationale for VIP request

To:

Cc: IPM at Mission (if an H&C case or a category 11 VIP)

Subject: High Priority Screening Request

Type of security screening request (VIT)	Email information
Rationale for VIP or H&C screening request	**To:** **Subject:** High Priority VIP or H&C Process Requested: UCI <12345678> **Body of e-mail:** **Name:** <Frank Loves Wheat> **DOB:** <YYYY/MM/DD> **UCI:** <12345678>

	For VIP cases (except category 11): This individual is described in category <X> of the VIP security screening procedures. He/she is the <Position Title> for <Country X> and will be travelling to Canada from <date> to <date> in order to <purpose of travel>. **For requests under VIP category 11 or on the basis of H&C:** Please provide a detailed rationale to explain the H&C element or why the individual is determined to be a VIP or within the national interest and therefore requires screening outside of regular service standards. This rationale should include the applicant's reason for travel and travel dates.

- If the applicant falls under the VIP category, the case will be processed within 48 hours (two working days in Ottawa), and a reply provided to the requestor. This will provide the visa office with the information required to continue processing the VIP case. If the applicant does not fall under the VIP category, the NSSD will notify the visa office immediately that normal processing will apply.
- There will be times when screening partners may require additional information or will require additional time. When this is the case, the NSSD will communicate with the visa office.
- The VIP process can be requested when an application is on hold.

10.6 Security screening request (VIT) after a TRV has been issued

If, after a TRV has been released to the applicant, a visa officer becomes aware of information that could change the assessment and render the applicant inadmissible to Canada, the NSSD should be contacted via _____ or the after hours Border Operations Centre a as well as Case Management Branch at IRCC via RCC officers should be prepared to provide as much information as possible on the person(s) concerned.

10.7 Service standards for screening temporary resident applications

The service standards for processing screening requests are as follows:

Temporary Resident Applications	Service Standard (for 80% of cases)
Urgent requests include: o National interest cases; and, o Cases based on humanitarian and compassionate grounds.	48 hours (excluding weekends)

VIP Processing	48 hours (excluding weekends)
	5 working days
	10 working days
Applications involving lookouts also fall under Tier 1 requests.	
Pre-diplomatic appointment	10 working days
Tier 2 requests –Canadian visa offices **in all other countries,** unless specific arrangements have been established between IRCC, the NSSD and screening partners to permit accelerated processing.	20 working days

Note: 'Working days' are based on the work week at National Headquarters (NHQ) in Ottawa, Canada. The work week starts Monday and ends on Friday (Eastern Time). Statutory holidays observed at NHQ do not count as working days.

Note: The NSSD screens approximately 50,000 temporary resident cases per year. In order to ensure due diligence and to address all areas of potential concern, security screening requests are not routinely expedited.

10.8 HOLD on cases

If, for any reason, the NSSD cannot coordinate a final response on a given temporary resident application within the allotted processing time, the NSSD will place the case on hold. The Security Sub Activity Status in GCMS will be set to "Hold"; if GCMS is not available NSSD will send an email to the originating visa office.

A hold message is an indication that initial concerns have been identified and that further research is required to establish a recommendation on admissibility. If a hold message is sent, officers should wait for additional information before making a final decision on the application.

Note: Regardless of whether the NSSD or screening partners request that a hold be placed on an appplicaton, the NSSD will coordinate and forward responses to visa offices on all cases and will be solely responsible for lifting holds. Officers receiving a message directly from CSIS to lift a hold should consult with the NSSD prior to issuing a visa.

10.9 Procedures when security screening service standard has been exceeded

Visa offices should receive an automated response for all cases.

If GCMS is not available, security screening requests may be transmitted If a security screening request is sent by e-mail using the VIT template, and no response or request for hold from the NSSD has been received within the allotted processing time, officers should refer to the following instructions:

Until further notice, **or until the indicator review has been completed on any given country**, IPMs are authorized to exercise discretion in expediting the finalization of applications that have exceeded the standard 10 working day processing time, regardless of the new service standards outlined above, in certain defined circumstances. These measures are temporary and internal. Applicants and stakeholders are not to be apprised of these interim measures, nor should visa offices alter their normal workflow to accommodate them.

- **New applications**

Visa offices should continue to apply the screening indicators outlined in the indicator manual. Individuals should be referred for security screening as per standard procedures. Applications that do not meet eligibility requirements from the outset, or that will be refused for other reasons, should not be referred for security screening to the NSSD and/or screening partners.

- **Applications pending VIT response**

IPMs may exercise discretion in order to expedite the finalization of applications that have reached or exceeded the 10 working day processing standard. Provided that the VIT status in GCMS is "Received", an IPM may notify the NSSD at the CBSA of the intent to issue a visa within one working day (ET). The message should indicate the reason the IPM is of the view that the case be finalized in the absence of completed security screening result. The IPM's message will be retained in the Secure Tracking System (STS) as a record of this decision. IPMs should send the following message to the

- This case has passed the 10 working day service standard. We are seeking to expedite this application for the following reason (fill in as appropriate):

  a) Bilateral relations.

  b) High profile case.

  c) Urgent family matter.

  d) Other (explain).

- The IPM is satisfied that there are no apparent security concerns.

Within one working day (ET), the NSSD will update the status of the security screening request to 'Inconclusive' or respond to indicate that security screening is in progress.

If the status of an application is updated to 'Inconclusive', a visa officer may proceed to finalize the application according to established protocol.

However, it should be noted that when an inconclusive finding is sent, the validity for the screening result will not apply and the person must be screened again if he/she applies

In cases where the NSSD indicates that there are potential security concerns identified and admissibility may be an issue, the visa officer should wait for a response from the NSSD.

If there is no response from the NSSD within one working day (ET), an authorized GCMS user may cancel the security screening request in GCMS and proceed to finalize the application according to established protocol.

Officers should indicate in the Notes section of GCMS that the pending security screening request was cancelled. Cases with a security screening request status of 'In Progress' should not be cancelled to allow partners to complete research already undertaken.

10.10 Validity of screening results – temporary resident applications

Favourable	**NSSD**	**CSIS**
	•	
Non-Favourable	**NSSD**	**CSIS**
	•	
Inconclusive Finding, No Recommendation Required	**NSSD**	**CSIS**
	• (if the person re-applies at a later time, the application must be screened again).	

Note: Validity of security screening results applies to applications for temporary residence only. When a person submits an application for a different line of business (i.e. permanent residence) the case must be re-sent for security screening.

10.11 Additional information

- Validity of screening results applies to single and multiple-entry visas, provided that the purpose (type of application) remains unchanged.
- If an applicant re-applies for a single-entry or multiple-entry TRV within is of the favourable result, the favourable result is valid and the visa officer may issue a TRV

with a validity of up to rom the latest favourable result without re-screening the application, unless a new lookout has been entered since the applicant was last screened.

- All applications made after of the last security screening result must be screened again, if the application meets relevant indicators.

Note: Officers maintain the discretion to re-send an application for re-screening if they suspect that an applicant may be inadmissible under section(s) 34, 35, and/or 37 of IRPA.

10.12 Multiple-entry visas versus single-entry visas

Multiple-entry visas (MEV) for eligible nationals

Officers are to issue multiple-entry visas (MEV) for up to ten years, minus one month or the validity period of the passport minus one month, to all eligible applicants. Applicants indicators have been developed, (refer to IC 2, Section 5) and the applicant does not fall within screening indicators, may be issued a 10-year MEV, provided the applicant meets all other requirements. The same applies to applicants who are screened against the general indicators (refer to IC 2, sections 6, 7 and 8).

Note: Not all applicants are eligible for an MEV. The decision to issue an MEV rests with IRCC officers. For guidance on issuing TRVs, refer to the Program Delivery Instructions Guidelines for issuing single-entry or multiple-entry visas.

Multiple-entry visas for nationals

IC 2. Section 5) may be issued multiple-entry visas (MEV) with a validity of up to at the officer's discretion, when the screening result is favourable.

- Officers should, to the extent possible, obtain a copy of the individual's travel itinerary clearly indicating the name and details of the host and letters of acceptance to an educational institution or employment details, as applicable.
- For additional information, please refer to the IRCC Program Delivery Instructions Temporary residents: Guidelines for issuing single-entry or multiple-entry visas.

11. Screening guidelines for permanent resident applications

For a visual representation of the security screening process refer to Appendix C.

11.1 Sending security screening requests

When an officer suspects that the applicant may be inadmissible pursuant to section(s) 34, 35 and/or 37 of IRPA, but requires additional information or the application hits on

indicators, the officer sends a security screening request to the CBSA and screening partners via GCMS to request screening of an applicant's background.

- When sending a security screening request, officers must use the appropriate tab (eg. Security" – section 34) to (refer to Table 1 below for a complete list of options). GCMS also requires that officers include case details prior to sending the screening request.
- To make GCMS case notes and other relevant documents (e.g. police tables, military information tables, etc.) available to screening partners, the documents should be uploaded to 'Notes section' in GCMS under the relevant screening tab (e.g. Security, HIRV, organized crime), so that partners have access to this information in GCMS.

11.2 Section 34 record check versus comprehensive check

The security tab (type 34) in GCMS provides officers with the option to send applications for security screening via a 'record check' (set as default) or a 'comprehensive check'.

Note: A record check is a standard check that is conducted by CSIS for most inland applications for permanent residence,

Note: A comprehensive check is conducted by all security screening partners, including the CBSA.

INLAND APPLICATIONS FOR PERMANENT RESIDENCE ONLY

- IRCC officers must refer most applications for permanent residence that are made from within Canada to CSIS for a 'record check'. CSIS screens these applications to assess current or future threats pursuant to paragraphs 34(1) (a), (c), (d) and (f) of IRPA only and as defined in section 2 of the CSIS Act (refer to section 8.3, page 14: CSIS mandate).
- A 'No Reportable Trace (NRT)' or 'no security concerns' reply from CSIS in response to a 'record check'
- Prior to sending an application to CSIS via a 'record check', officers should also check the PR application against the indicators in the IC 2 indicator manual.
- PR applications that hit on an indicator and/or where an officer suspects that the applicant may be inadmissible should refer the application via a 'comprehensive check' as outlined in Table 1 below to ensure that the CBSA also screens the case.

OVERSEAS APPLICATIONS FOR PERMANENT RESIDENCE ONLY [INCLUDES CASE PROCESSING CENTRE OTTAWA (CPC-O]

- While sending security screening referrals as "comprehensive" checks is the preferred option, there may be cases for which a section 34 Record check is more appropriate, keeping in mind that Record checks only go to CSIS.
- CBSA only screen applications that hit on indicators as outlined in section 3 of the IC2. Applications that are referred for section 35 and 37 screening are screened by the CBSA.

- Applications that hit on an indicator and/or an officer suspects that the applicant may be inadmissible should be referred for security screening as outlined in Table 1 below.

TABLE 1: Sending a security screening request to the NSSD and screening partners:

The following table lists the various types of requests and security screening partners to whom screening requests for permanent resident applications should be sent:

Section of IRPA	Screening Values - GCMS	Criteria	Case goes to
34	Security Screening Record Check	• most inland applications	CSIS
34	Security Screening Comprehensive check	Inland and overseas applications that meet one or several of the following: • the applicant is subject to a lookout related to section 34 of IRPA; • the applicant meets one or more of the applicable screening indicators listed in the IC 2; • the officer suspects that the applicant may be inadmissible pursuant to subsection 34(1) of IRPA.	CBSA, CSIS
35	Human and International Rights Violations (HIRV)	• the applicant is subject to a lookout related to section 35 of IRPA; • the applicant meets one or more of the applicable screening indicators listed in the IC 2; • an officer suspects that the applicant may be inadmissible under section 35 of IRPA.	CBSA
37	Organized Crime	• the applicant is subject to a lookout related to section 37 of IRPA; • the applicant meets one or	CBSA

Section of IRPA	Screening Values - GCMS	Criteria	Case goes to
		more of the applicable screening indicators listed in IC 2; • an officer suspects that the applicant may be inadmissible under section 37(1) of IRPA.	

Note: Regardless of the reason for referral, the NSSD will screen all cases for concerns pursuant to sections 34, 35 and 37 of IRPA, provided that a comprehensive check was requested.

Note: When the NSSD provides an inadmissibility recommendation for an inland PR application, the recommendation is sent to IRCC as well as the applicable CBSA regional office.

11.3 Service delivery standards for screening permanent resident applications

Type of Permanent Resident Application	Service Standard(for 80% of cases)
- Permanent resident – Urgent Protection Processing/Urgent	- (excluding weekends)
- Permanent resident application	- 110 calendar days

11.4 Validity of screening results (permanent resident applications)

The validity period for screening results provided by the NSSD and screening partners is as follows:

Favourable	**NSSD**	**CSIS**
	• valid for	
Non-Favourable	**NSSD**	**CSIS**
	• valid for	• valid for
Inconclusive Finding, No Recommendation	**NSSD**	**CSIS**
	• d (if the individual re-applies at a later time, the applicant must be screened again).	

Required	

Note: Validity of security screening results applies to applications for permanent residence only. When a person submits an application for a different line of business (i.e. temporary residence) the case must be re-sent for security screening.

12. Screening guidelines for front end security screening of refugee protection claimants

12.1 Front end security screening background

The purpose of front-end security screening of refugee protection claimants is to maintain the integrity of the refugee determination program and to enhance Canada's security by identifying potential security cases as early as possible.

To this end, all claims for refugee protection made at ports of entry (POE) and inland offices are sent to the NSSD at the CBSA for security screening for inadmissibility pursuant to sections 34, 35 and/or 37 of IRPA. CSIS screens claims and conducts a threat assessment pursuant to section 2 of the CSIS Act.

12.2 Preparing security screening requests

Officers who are responsible for refugee intake at the POE and inland offices should ensure that claimants provide adequate responses to all security related questions in the Schedule A- Background (IMM5669) form prior to sending the information to the CBSA and screening partners.

12.3 Inland claims (IRCC)

Officers are to send security screening requests for in-land refugee protection claims to the CBSA via GCMS as per established procedure.

12.4 POE Claims (CBSA referrals)

CBSA officers at POEs should send all requests for security screening via GCMS and upload all intake documents according to established procedures.

12.5 Service standards

Security screening service standards pertaining to refugee claims correspond with legislated timeframes and are calculated from the date of the eligibility determination as follows:

Type of Claim for Refugee Protection	NSSD Service Standard (for 80% of cases)
Claims made at an inland office by individuals coming from]	25 working days
Claims made at a POE by individuals coming from a	40 working days

	55 working days

Note: 'Working days' are based on the work week at National Headquarters (NHQ) in Ottawa, Canada. The work week starts Monday and ends on Friday (Eastern Time). Statutory holidays observed at NHQ do not count as working days.

12.6 Ineligible claimants

Claimants who are ineligible to have their claims referred to the Refugee Protection Division (RPD) of the Immigration and Refugee Board (IRB) are not referred to the NSSD for front end security screening.

12.7 Identity verification for claimants who are in detention

IRCC and CBSA officers may refer a claimant for security screening; however, the CBSA will not complete the screening process until the identity of the claimant has been established.

12.8 Abandoned Claims

In the event that a claimant abandons the claim, the CBSA will cease screening efforts and provide a 'no recommendation required' result.

12.9 Screening results

All security screening results are entered into GCMS. The CBSA regional offices (National Security Hearings Unit) will decide whether or not to refer the file to the Immigration Division for an admissibility hearing or intervene at a claimant's refugee protection hearing at the RPD.

Note: For information on processing refugee protection claims, please consult the Program Delivery Instructions for Processing Claims for Refuge protection in Canada.

13. Global Case Management System (GCMS)

GCMS contact information

IRCC

When encountering system problems while attempting to send security screening requests via GCMS, an email should be sent to by an authorized individual with a detailed description of the problem.

CBSA

When encountering system problems while attempting to send security screening requests via GCMS, an email should be sent to by an authorized individual with a detailed description of the problem.

14. Security screening interviews to obtain additional information (for all streams)

If officers do not have enough information to establish reasonable grounds to believe that an individual is inadmissible under section(s) 34, 35 and/or 37 of IRPA, officers may conduct an interview to obtain additional information.

Note: For additional information on conducting interviews, please refer to Appendix E of this manual chapter.

14.1 Consulting and inviting partners to interviews

Screening partners may be invited to participate in interviews, if visa officers consider it appropriate and where there is partner interest and availability. **It is important to note that when a partner agency assists in conducting an interview, the visa officer should remain the lead during the interview.**

The role of a partner agency in a joint interview is to provide the examining officer with timely verbal advice regarding national security or organized criminality. Visa officers should always take the lead and are solely responsible for conducting the interview and for taking notes. Section 16(1) of IRPA requires applicants to answer truthfully to questions directly related to the immigration process. This may not be the case if questions are asked by a partner agency during an immigration interview.

For guidance on the application of section 16 of IRPA, officers should refer to ENF 2, Evaluating Inadmissibility, section 11.2 and the Operational Bulletin: CBSA OB PRG-2013-37: "Coming into Force of Bill C-43 – Obligations for certain persons making an application under the *Immigration and Refugee Protection Act* (IRPA)."

15. Screening results returned to IRCC (for all streams)

15.1 Inadmissibility recommendations (CBSA)

For cases that the NSSD received via GCMS, the inadmissibility recommendation will be provided through GCMS (this applies to record checks as well as to comprehensive checks).

Once the NSSD has completed research and analysis with respect to a particular case, an admissibility recommendation is prepared and returned to the appropriate visa office or IRCC inland office as the case may be.

Favourable:

A "Favourable" recommendation applies in circumstances where the NSSD and/or screening partners are of the opinion that there are **insufficient** reasonable grounds to believe the applicant is inadmissible pursuant to section(s) 34, 35 and/or 37 of IRPA.

Non-Favourable:

A "Non-Favourable" recommendation applies in circumstances where the NSSD and/or screening partners are of the opinion that there are **sufficient** reasonable grounds to believe the applicant is inadmissible pursuant to section(s) 34, 35 and/or 37 of IRPA.

"Non-Favourable" also applies when a case is referred within the validity period of a previous inadmissible assessment.

Inconclusive Findings:

An "Inconclusive Finding" recommendation applies in the following situations:

- anytime that the NSSD and/or screening partners are unable to complete the assessment of a case because the visa office or the applicant did not provide sufficient information when further details were requested.

No Recommendation Required:

The "No Recommendation Required" recommendation applies in the following situations:

- the application was withdrawn or cancelled;
- IRCC made a final determination prior to the completion of security screening;
- the case is a duplicate referral or was referred in error;
- the applicant underwent security screening previously and the case was referred within the validity period of a recommendation that was initially "Favourable"; or,
- the applicant is under the age of 18, unless special circumstances that require screening exist (i.e. the officer suspects that the child was a former child soldier) .

16. Admissibility determination (IRCC)

The delegation of authority to issue a temporary or permanent resident visa rests with IRCC officers. If an IRCC officer reviews an inadmissibility recommendation provided by the CBSA and does not agree with the assessment, the officer should proceed as outlined in section 17 below.

In cases where a temporary or permanent resident visa is issued despite a non-favourable recommendation,

If the non-favourable recommendation provided by the CBSA includes information that was provided by (IRCC officers should also advise Client Liaison, Security Screening Branch, CSIS via

17. Contrary outcomes

The following instructions were developed to ensure that IRCC decision makers undertake a final consultation with security screening partners before making a final decision on cases where the final decision is contrary to the recommendation provided by the CBSA.

Note: These instructions apply to overseas cases. Instructions for inland cases are under development.

17.1 Definition:

- IRCC has received a non-favourable inadmissibility recommendation from the CBSA and the IRCC decision maker, after taking into consideration all available information, wishes to issue a visa with no finding of inadmissibility; or
- IRCC has received a favourable recommendation from the NSSD and the IRCC decision maker wishes to refuse the visa pursuant to inadmissibility under section(s) A34, 35 or 37 of IRPA.

The definition of "contrary outcome" does **not** apply when:

- An applicant was determined to be inadmissible pursuant to sections 34, 35 or 37 of IRPA and was (or will be) issued a visa under one of the remedies listed in section 21 of this manual.

17.2 'Contrary outcome' scenarios

After considering all available information, IRCC decision makers may determine that limited weight should be given to an inadmissibility recommendation provided by the CBSA, which in turn may result in a favourable or unfavourable admissibility determination, as the case may be.

The most likely reasons contributing to contrary outcomes include, but are not limited to the following scenarios:

- The information provided in the inadmissibility recommendation is insufficient to support allegation(s) pursuant to section 34, 35 or 37 of IRPA.
- Classified information that can not be released to the applicant or used in court proceedings was provided in the inadmissibility assessment, which would limit the IRCC decision maker in preparing a strong refusal that can be defended in a court of law.
- The IRCC decision maker interviewed the applicant, who provided additional information related to a potential inadmissibility. The decion maker was satisfied that the applicant is not inadmissible and proceeded favourably.
- The inadmissibility recommendation included a possible error based on fact and/or interpretation of the law.

- New information that may/will impact the inadmissibility recommendation was presented to the IRCC decision maker (

17.3 Instructions for processing contrary outcome cases at visa offices and at the Case Processing Centre-Ottawa

It is recognized that visa offices often communicate directly with security partners in 'contrary outcome' type cases. The following instructions serve to standardize the process and outline steps that must be followed by IRCC officers and security screening partners before a 'contrary outcome' case can be concluded.

Note: IRCC officers are the final decision makers on visa issuance. The instructions below should not be construed as 'fettering' the final decision. Should a potential 'contrary outcome' not be resolved through the process outlined below, the decision maker will proceed with the admissibility determination.

The following procedures have been developed to establish a dynamic consultation process that ensures that reasonable efforts are made among partners to resolve contrary admissibility opinions before an admissibility decision is rendered. This process also ensures that decision makers have all the necessary information to make a well informed decision.

Before making a decision on a potential 'contrary outcome' case, IRCC decision makers will provide the CBSA with all available additional/new information that could result in changes to the inadmissibility recommendation.

IRCC's role in communicating a potential 'contray outcome'

If the content of the message is SECRET, it must be sent via C5:	If the content of the message is NOT SECRET, it can be sent via email:
TO: CC: _____ _____ _____ _____ _____	TO: _____ _____ _____ _____ _____ _____

[2] NSSD will re-assess the case and if appropriate, change the inadmissibility recommendation based on the new information and the case is no longer considered a 'contrary outcome'.

SUBJECT: Potential Contrary Outcome "UCI, "CLIENT NAME"	**SUBJECT:** Potential Contrary Outcome, "UCI, "CLIENT NAME"

The IRCC decision maker must include the following information in the email message:

1. Client's full name
2. Case #
3. UCI #
4. STS #
5. Name of the IRCC decisions maker
6. Applicable subsection of 34, 35 and/or 37 of IRPA
7. Inadmissibility recommendation received from the CBSA.
8. General reason(s) for the contrary opinion of the IRCC decision maker:
   - Not satisfied that evidence is sufficient to support allegation;
   - Not satisfied sufficient releasable evidence to support allegation;
   - Possible error in fact and/or law;
   - New information available;
   - Detailed explanation for 'contrary outcome' opinion.
9. Detailed explanation and rationale for 'contrary outcome' opinion. (Please note that a more detailed explanation will make it easier for the CBSA and other security screening partners to address specific concerns of the IRCC decision maker.)

NOTE: If the applicant meets the definition of a VIP, please follow the instructions set out in Section '10.5 Very important Person VIP – Priority Security Screening Procedures' of this manual.

Note: If the message is sent via IRCC decisions makers should send a follow-up email to advise that a message was sent as follows:

TO:

SUBJECT: Potential Contrary Outcome, "UCI", "CLIENT NAME"

17.4 The CBSA's role

The CBSA acts as the lead agency with respect to 'contrary outcome' cases. As per the procedures outlined in section 17.3 above, IRCC advises the CBSA of potential 'contrary outcomes' cases; the CBSA in turn informs screening partners. Taking into consideration information received from security screening partners, the CBSA provides a response to IRCC within established timelines as follows:

CBSA response times

Once advised by IRCC of a possible 'contrary outcome', the CBSA (and partner agencies) agree to respond within the following timeframes:

Temporary Resident Applications	Permanent Resident Applications
Within 2 working days: The CBSA acknowledges receipt of the notification;	**Within 2 working days:** The CBSA acknowledges receipt of the notification;
Within 5 working days: The CBSA provides a final reply	**Within 10 working days:** The CBSA provides a final reply.
1. As soon as the CBSA is notified of a potential 'contrary outcome' case by IRCC, the CBSA advises security screening partners to allow for adequate processing time. - For section 34 cases, the CBSA sends an urgent notification e-mail to ; including instructions for the email to be forwarded to	1. As soon as the CBSA is notified of a potential 'contrary outcome' case by IRCC, the CBSA advises security screening partners to allow for adequate processing time. - For section 34 cases, the CBSA sends an urgent notification e-mail to including instructions for the email to be forwarded to
2. The CBSA notifies IRCC within the first day, if it is anticipated that the deadline of 5 working days will not be met. Requests for extension must be submitted at this time.	2. The CBSA notifies IRCC within the first day, if it is anticipated that the deadline of 10 working days will not be met. Requests for extension must be submitted at this time.
The CBSA provides a final recommendation to the decision maker within 5 working days, including additional information received	3. The CBSA provides a final recommendation to the decision maker within 10 working days, including

Temporary Resident Applications	Permanent Resident Applications
from screening partners. Should the initial inadmissibility assessment remain the same, the CBSA will provide IRCC with a rationale by email via	additional information received from screening partners. Should the initial inadmissibility assessment remain the same, the CBSA will provide IRCC with a rationale by email via

*Note: 'working days's are based on the work week at National Headquarters (NHQ) in Ottawa, Canada. The work week starts Monday and ends on Friday (Eastern Time). Statutory holidays observed at NHQ do not count as working days.

17.5 Communicating the decision

The IRCC decision maker reviews and considers the final inadmissibility assessessment provided by the CBSA. Prior to making a decision that is contrary to the final inadmissibility assessment, the decision maker will engage IRCC National Headquarter (NHQ) by sending an email to the following email addresses:

To:

CC:

This will allow IRCC NHQ to engage in discussions with the CBSA in order to mitigate potential bilateral irritants and determine the appropriate way forward.
IRCC NHQ will communicate the outcome of the discussions with the CBSA to the visa office within 10 working days, at which time the case can be finalized, unless Case Management Branch (IRCC) requests that the case be put on hold.

Removal of lookouts In the case of a contrary outcome, the prerogative to retain or remove a lookout rests with the CBSA. The CBSA will inform all key players of the decision and provide instructions to ports of entry on the review of case notes that pertain to IRCC's admissibility determination and CBSA's inadmissibility recommendation.

17.6 Additional references

As some cases that lead to contrary outcomes may also be high-profile, complex, sensitive or contentious cases and may result in bi-lateral irritants, officers are reminded to review the following related to instructions while assessing the case:

- Section 18.1 below: Reporting high profile, complex, sensitive or contentious cases
- Section 10.5 above: Very Important Person (VIP) – priority screening procedures
- Program Delivery Instructions for Reporting high profile, complex sensitive or contentious cases

Note: Notwithstanding a final determination by an IRCC decision maker to issue a temporary or permanent resident visa, CBSA BSOs must be satisfied that an individual is not inadmissible before granting entry to Canada. [Status and authorization to enter: Subsection 21(1) of IRPA for permanent residents and subsection 22(1) for temporary residents].

18. Refusals under section(s) 34, 35 and/or 37 of IRPA

If the IRCC officer agrees with an inadmissibility recommendation that a refusal is warranted, the application should be refused, and the applicant advised as per current protocol. The specific section of the Act should be referenced, but not spelled out. **Classified information, including CSIS information must not be included in procedural fairness or refusal letters.** Prior to issuing a refusal letter, procedural fairness letters should be sent to clients for concerns pursuant to section(s) 34, 35 and/or 37 of IRPA as per current protocol.

Before an IRCC officer issues a refusal letter or procedural fairness letter under inadmissibility provision(s) 34, 35, and/or 37 of IRPA, an IRCC manager must review the letter before it is sent to the client, with a view towards the elimination of language that may give rise to bilateral irritants.

18.1. High profile, contentious and sensitive cases

NHQ (IRCC and CBSA) should be notified of all high profile, contentious or sensitive cases (overseas and inland) that will be refused under section(s) 34, 35 and/or 37 of IRPA.

The following recipients should be copied:

- Immigration Program Manager (if applicable);
- the current Director General and Senior Director of Case Management Branch and the Office of the Assistant Deputy Minister, Operations);
- CBSA via]

Field Code Changed

- the relevant IRCC International Region (IR) geographic desk, and;
- for refusals under section 34 of IRPA, officers should also notify CSIS via

Officers should review the existing instructions related to the management of high-profile, contentious and sensitive cases in the Program Delivery Instructions for Reporting high profile, complex sensitive or contentious cases.

19. Responses to a refusal

IRCC officers are responsible for responding to any representations or questions related to a refusal.

Officers may consult IRCC's Litigation Management Division of Case Management Branch (CMB) at who will assist on issues related to litigation and procedural fairness.

20. Lookouts/alerts

According to the Multiple Borders Strategy, lookouts and alerts must be provided to the NSSD and IRCC officers, whether stationed in Canada, at ports of entry or overseas, so that officers can consider the information and/or intelligence before them and take appropriate action. In accordance with this strategy:

- Each time the NSSD provides an inadmissibility recommendation to a visa office, it should also create an EII lookout in the Integrated Customs Enforcement System (ICES), for the benefit of BSOs who may encounter this individual.
- Should a visa office decide to use a remedy (refer to Section 21 below) to enable the inadmissible applicant to travel to Canada, the visa office should verify if the lookout was silenced in the system. In cases where the lookout was not silenced, the visa office should contact the NSSD via email at or the Border Operations Centre at (613) 960-6001 to ensure that the lookout is silenced for the validity period of the remedy.
- The final decision as to whether or not the EII lookout is silenced rests with the CBSA.

21. Remedies

21.1. Remedies to facilitate temporary residence

National Interest Temporary Resident Permit (NI-TRP) and Public Policy Temporary Resident Visa (PPTRV)

In cases where national interest considerations have been identified, notwithstanding the fact that an officer establishes reasonable grounds to believe that a foreign national is inadmissible to Canada under section(s) 34, 35, and/or 37 of IRPA, a National Interest

Temporary Resident Permit (NI-TRP) or a Public Policy Temporary Resident Visa (PPTRV) may be issued for a specific purpose and duration.

Both the NITRP and PPTRV require a letter of national interest to be submitted by the inviting department sponsoring the individual's visit to Canada.

Procedures related to the issuance of PPTRVs and NI TRPs are updated regularly. For instructions on processing cases involving PPTRV and NITRV, please refer to the Program Delivery Instructions for Temporary Resident Permits (TRPs) and OB 463: National Interest Temporary Resident Permits and Public Policy Temporary Resident Visas.

21.2. Remedy to facilitate permanent residence

Applications for Ministerial Relief (MR)

For guidance with respect to Ministerial relief applications, please contact the CBSA Ministerial Relief Unit (MRU) via I

22. Other related processes

22.1. The *Foreign Missions and International Organizations Act*

The *Foreign Missions and International Organizations Act* (FMIOA) allows the Governor in Council to extend privileges and immunities to an international organization, its officials and to representatives of a foreign state that is a member of, or participates in, an international organization headquartered in Canada or that holds meetings or conferences in Canada (e.g., the International Civil Aviation Organization).

Since the privileges and immunities are granted by order of the Governor in Council, the respective order pertaining to the organization, meeting or event will specify the privileges and immunities accorded to the representatives, officials, experts or other classes of persons. For this reason, any event where an order has been issued under the FMIOA will be noted in the "Comments" section of the event notice and a link to the relevant Order in Council (OIC) will be provided whenever possible.

Visa officers processing TRV applications for persons coming to Canada to participate in a special event should consult the Special Event Notices located within IRCC's Program Delivery Pages or contact CMB via [illegible] l/or for guidance.

All visa applications for participants covered by the FMIOA must be processed expeditiously and without charge or restriction. In other words, the visa requirement itself should not become an impediment for the person's travel and entry to Canada.

22.2. FMIOA security screening and advising NHQ

- IRCC officers processing TRV applications for persons coming to Canada to participate in a special event should verify if specific instructions for the particular event were issued via a Special Event Notice and follow the instructions provided.

- IRCC officers should also consult the Program Delivery Instructions for Reporting high profile, complex sensitive or contentious cases. Officers who require additional information may contact CMB via] IRCC officers should refer cases for which they have admissibility concerns pursuant to section(s) 34, 35 and/or 37 to the NSSD for VIP/Urgent screening (refer to section 10.4 of this manual).
- Individuals who meet eligibility criteria and require a visa to come to Canada should be issued a Temporary Resident Visa (TRV) not a Temporary Resident Permit (TRP), even if they are inadmissible pursuant to sections of 33-43 of IRPA.
- Should a TRV be issued to a person who is inadmissible pursuant to section(s) 34, 35 and or 37 of IRPA, officers are to notify the NSSD via email at and follow instructions in the Program Delivery Instructions for Reporting high profile, complex sensitive or contentious cases indicating that the person is covered by an Order under the FMIOA and include the name of the event.
- If an applicant who is covered by the FMIOA is subject to a lookout in GCMS, officers must contact the CBSA (Lookout Team and NSSD), if the visa office decides to issue a visa. The email should include the following information:
  - **TO:**]
  - **CC:**]
    - **Name**: First, LAST
    - **DOB**:
    - **GCMS UCI**:
    - **Anticipated date of arrival**:
    - **Anticipated date of departure**:
    - **Type of Visa issued**:
    - **Type of Exemption**: FMIOA

Note: Should applicants apply in the future under different circumstances (i.e., non-FMIOA), the application must be referred to the CBSA via GCMS for security screening as per the procedures outlined in this manual.

22.3. Port of entry screening

Note: When conducting immigration examinations at the port of entry (POE), Border Services Officers (BSO) may use the guidelines set out in ENF 4: Port of entry examinations for guidance on issues of admissibility. For information on who to contact at NHQ for information on inadmissibility pursuant to section(s) 34, 35 and/or 37 of IRPA, please refer to Appendix F of this manual chapter.

23. Seizure of documents

Note: If, during the course of a port of entry examination, documents or records are collected or seized in accordance with section 15(3) of IRPA,
accordance with section 8(2)(a) of the Privacy Act.[3] Seized documents should be sent to:

24. Inland security screening

24.1. Extension or change of status

Note: For guidance on which applications should be referred for security screening, refer to sections 9, 10, and 11 of this manual.

24.2. Work and study permits issued in Canada and overseas

Foreign nationals subject to security screening procedures may be issued work/study permits or granted extensions to their authorizations for an appropriate duration, provided that screening and normal temporary resident and work/study permit requirements (including Employment and Social Development Canada (ESDC) labour market impact assesments) are met.

Applications from individuals holding valid Canadian work or study permits (IMM 1442) who apply at visa offices abroad to obtain new visa counterfoils to return to Canada to continue their employment or study, will be processed as "workers" and "students" as per the screening requirements of this manual.

The validity of visa counterfoils issued to students and workers should be consistent with the guidance set out in the Program Delivery Instructions for TRs. While work and study permits may be issued for the length of time appropriate to the permit (i.e., for the duration of the program of study), possession of these permits does not eliminate the need for security screening prior to re-entering Canada.
must have security screening requests (VIIS) resubmitted after the initial screening as outlined in section 18. These applications are subject to normal screening procedures.

[3] Section 8(2) states that 'Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

Appendix A Protected and classified information

	Protected B	Secret	Top Secret
Description	Medium to Serious Injury if compromised. Unauthorized release could cause serious injury to an individual, organization or government: • Prejudicial treatment • Loss of reputation or competitive edge	Unauthorized release could cause an injury to the national interest	Unauthorized release could cause extremely serious injury to the national interest
Examples	• Personal information/ Biographical data • Medical/Psychiatric/ Bank Records • Competitive position of a third party • Trade secrets of a third party • Criminal information • Performance evaluations • Religious or political beliefs • Information received "in confidence" from other government organizations • API/PNR information • Social insurance number	• Minutes or Records of Cabinet Committees • Draft legislation • Strategies, tactics relating to international negotiations • Case files with national security implications	• Important and significant negotiations • Vital law enforcement and Intelligence matters • Information classified by CSIS & RCMP regarding strategic plans, criminal or security threats
Physical Storage	• Operations Zone is defined as an area where access is limited to personnel who work there and to properly escorted visitors – example – Typical Government	• Approved security container (file cabinet or safe) with approved combination lock in a Security Zone. • "Security Zone" is defined as an area where access is	• Approved security container (safe) with approved combination lock in a Security Zone. • Note: when determined by a TRA and operational

	Protected B	Secret	Top Secret
	open office space	limited to authorized, appropriately screened personnel and authorized and properly escorted visitors.	requirements, Top Secret material may be segregated and controlled within a closed community within a High Security Zone. • "High Security Zone" is defined as an area where access is limited to authorized, appropriately screened personnel and authorized and properly escorted visitors
Electronic Storage	• Common or shared drive – (G:\) (H:\) • Portable media – Laptop (programmed with Safeguard Easy) • Blackberry – Encrypted with controlled access (User ID) not enabled with PIN to PIN communications • Diskettes, USB sticks, compact disks (labelled) • When using portable media, information stored on these items must be transferred to Corporate network drives and removed from portable media • Portable Items in an approved security container – locked when not in use	• Contact Corporate Security and Internal Affairs • Requires Type I Crypto • Missions, Consult with Security Officer	• Specialized Secure Top Secret network (Contact Corporate Information Security) • No Blackberry • For Missions, Consult with Security Officer • Portable media in a dial safe, in a high security zone. Locked when not in use

	Protected B	Secret	Top Secret
Transmittal – Mail	**For both Internal and External Mail:** • Mark inner gum-sealed envelope "Protected B" – "to be opened by addressee only" • Unmarked outer gum-sealed envelope • Internal and regular mail or if tracking is preferred, it can be sent by Priority Post	• 2 gum sealed envelopes • Mark on inner envelope: "Secret" – "to be opened by addressee only" • Unmarked outer gum-sealed envelope • Include Transmittal Note (GC44) • Notify recipient before sending and keep a record of the document • Deliver using agency mailroom	• 2 gum sealed envelopes • Mark on inner envelope: "Top Secret" – "to be opened by addressee only" • Unmarked outer gum-sealed envelope • Include Transmittal Note (GC44) • Notify recipient before sending and keep a record of the document • Deliver using agency mailroom
Electronic Transmission (Email & Fax)	• Email – PKI encryption or other approved encryption method • Secure "Protected" Facsimile Network consists of Fax equipped with fax encryption device (e.g. MOBIUS, CERTIFAX, SK5000)	• Must not be emailed. • Secure fax (connected to a COMSEC Telecommunication Equipment) • To the Missions – Consult with Security Officer	• Must not be emailed. • Secure fax (connected to a COMSEC Telecommunication Equipment)
Print	• Network Printer with PIN or local Printer	• No network Printing • Dedicated Local Printer in restricted area	• No network Printing • Dedicated Local Printer in restricted area
Telephone Communication	• Regular land-line phone communication in Canada/US • COMSEC Telecommunications Equipment outside	• Connected to a COMSEC Telecommunication Equipment	• Connected to a COMSEC Telecommunication Equipment

	Protected B	Secret	Top Secret
	Canada/US including Missions		
Paper Destruction	• Approved Paper Shredder • Consult with Regional Security or Corporate Security and Internal Affairs Division	• Approved Paper Shredder must perform a crosscut operation with at least two, cross-oriented blade sets. • Consult with Regional Security or Corporate Security and Internal Affairs	• Approved Paper Shredder must perform a crosscut operation with at least two, cross-oriented blade sets. • Consult with Regional Security or Corporate Security and Internal Affairs
Disposal	• To securely delete all data on hard drive, with an approved disk sanitization utility (contact Corporate Information Security) **Note:** Portable media including hard disks may require physical destruction (contact Corporate Information Security)	• Delete securely with an approved disk sanitization utility and contact Corporate IT Security. • **Note:** Portable media including hard disks will require physical destruction (contact Corporate Information Security). • Missions – give media to Systems Administrator for destruction	• Delete securely with an approved disk sanitization utility and contact Corporate Information Security • **Note:** Portable media including hard disks will require physical destruction (contact Corporate Information Security). • Missions – give media to Systems Administrator for destruction
Personnel Security Screening Requirement	**Reliability Status**	**Secret**	**Top Secret**

Appendix B – screening tools

1. The following manual chapters* provide additional guidance related to screening:

IC 2	• Indicator Manual (available in hard copy only)
ENF 2/OP 18	• Evaluating inadmissibility
ENF 4	• Port of entry examinations
ENF 28	• Ministerial Opinions on Danger to the Public and to the Security of Canada
ENF 18	• War Crimes and Crimes Against Humanity
OP 1	• Procedures (provides general information on overseas processing)
OP 6 (Program Delivery Instructions)	• Federal Skilled Worker (FSW) Class applications
OP 7a	• Quebec Skilled Worker Class applications
IP 4	• Processing Live-in Caregivers in Canada
IP 5 (Program Delivery Instructions)	• Immigrant Applications in Canada made on Humanitarian or Compassionate Grounds
IP 7	• Entrepreneur Program
IP 8	• Spouse and Common-law partner in Canada Class
IP 11 (Program Delivery Instructions)	• Anti-fraud
PP 4	• Processing Protected Persons' in-Canada Applications for Permanent Resident Status

2. Systems

IRCC officers have access to a number of systems and tools that assist them in making admissibility determinations.

While some systems have shared access, the NSSD and screening partners rely on additional tools and systems to assess temporary and permanent resident applications referred by IRCC for security screening.

The following systems are available to decision-makers in Canada and overseas. These systems do not represent an exhaustive list of databases and tools available to the NSSD and partners to conduct security screening.

2.1. The Global Case Management System (GCMS)

Note: The Field Operational Support System (FOSS) was decommissioned in November 2015.

Essential information including client histories and prior enforcement action, is now available in the Global Case Management System (GCMS). GCMS also includes important indicators regarding potential threats and inadmissibilities, which may assist officers in making admissibility determinations.

- All officers responsible for screening foreign nationals must check GCMS prior to sending a screening request to partners.
- Checks must be conducted regardless of whether the client is known to the processing office or whether previous systems checks were non-resultant. These checks are important since information in the systems may change quickly.
- **The CBSA maintains an extensive number of EII and lookouts. These lookouts are important tools available to officers in making well-informed decisions. It is important to indicate in a screening request sent to the NSSD, the presence of lookouts relating to a particular individual.**
- To accurately reflect the action taken on a particular file, officers must record system checks and the results in GCMS. These remarks will assist those officers responsible for conducting follow-up activities on a particular person to quickly identify what actions have been taken thus far.

3. Open source research

Officers are encouraged to conduct open source research using the internet, which can provide significant insight on organizations, country conditions and other information to support admissibility decisions.

3.1. Assessing internet-based sources for reliability

The internet is an excellent research tool that is generally fast and easy to access. However, it is important to consider the reliability of sources. For example, Wikipedia is not considered a reliable source.

Officers should use their own judgment as to whether a particular site is reliable, keeping in mind that when making an admissibility determination on a specific application, IRCC officers will have to substantiate that the person(s) is (are) inadmissible and, in some cases, defend the decision in a court of law. To this end, when making reference to information from a specific website, officers should record the website link as well as the date on which they accessed the website.

3.2. When evaluating if a website is reliable, officers should consider the following:

1. **Authority and reputation of the author**
   a. Who are the authors and/or publishers of the website?
   b. How reputable are the authors and/or publishers? Are they subject matter experts?
   c. Is the site the original site of a known paper periodical, newspaper or organization?
   d. Is information about the authors and/or producers easily available on the site itself?
   e. Are contact details, i.e. email and postal addresses provided on the site?
   f. How is the site funded (source of financing?) (goes to bias).

2. **Scope and intended audience**
   a. What is the intended subject?
   b. Who is the intended audience (target/purpose of the site)?

3. **How does the source compare to other sources?**
   a. How does the source compare to other sites dealing with similar subject matter? Compare/contrast depth of how subject matter is treated.

4. **Coverage of subject**
   a. How complete and reliable is the information?
   b. What other resources (print and non-print) are available on the particular country you are researching?
   c. What is the relative value of the site in comparison to the range of information/resources available on the country you are researching?

d. Does the website cover the subject adequately?
e. Are there any links to additional information?

5. **Accuracy of information**
   a. Is the information accurate? (very important)
   b. Does the information have a research basis?
   c. Is the information supported by published research findings?
   d. Where doubt about credibility of the information exists, can you cross-reference the content/information with a more reliable source?
   e. Is the on-line version a complete document, or is it part of a document published on-line only prior to release of the work? I.e. excerpt of a larger document to be published in the future?
   f. Does the text follow basic rules of grammar, spelling, composition?

6. **Is the information current? – this is important when it comes to determining factors related to potential inadmissibility pursuant to sections 34, 35 and/or 37 of IRPA.**
   a. Is the information up-to-date? Recent? What is the date?
   b. How frequently and/or regularly is the information updated?

7. **Format of the source**
   a. Is the site accessed easily?
   b. How easy is it to navigate through the site and download documents?
   c. Are back-issues available? Does the site include an archive?
   d. Does the site include an internal search-engine?
   e. Is the information contained on the site in the public domain or are their copyright restrictions?

8. **Some examples:**
   a. Assess each of the following websites using the key questions listed above.
   b. Note anything that may detract from the reliability of the website.
   c. Form an opinion as to whether or not the website is reliable.

3.3. Using search engines effectively:

Check out the advance search pages of FAQs

Refer to:
UC Berkeley, Teaching Library Internet Workshops. "The Best Search Engines."
(http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/SearchEngines.html)

Choosing key words:
- Start very broadly and see what you get, or
- You can focus initially and expand to thematic searches

Specifying searches:
- Use quotation marks for phrases
- Use Boolean Operators (Or, brackets, and, not)
- Proximity tools

Dealing with transliteration:
- Vowels are a particular problem
- Try 'or' to include multiple spellings in search
- Use truncation where appropriate

3.4. Following are examples of reliable sources:

Canadian court decisions:

- Federal Court of Canada: Federal Court (Canada)
- Federal Court of Appeal: Federal Court of Appeal
- Supreme Court of Canada: Supreme Court of Canada
- CanLII - Canadian Legal Information Institute

Canadian government resources:

- Immigration and Refugee Board (IRB): http://www.irb-cisr.gc.ca
- Financial Transactions and Reports Analysis Centre of Canada - http://www.fintrac.gc.ca/
- Public Safety http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/index-eng.aspx

United States of America resources:

- Central Intelligence Agency (CIA) - https://www.cia.gov/library/publications/the-world-factbook/
- Federal Bureau of Investigation (FBI): http://www.fbi.gov/
- US Department of State : http://www.state.gov/j/ct/rls/crt/
- Open Source Centre (requires login): Open Source Center - Login

United Nations resources:

- RefWorld: http://www.refworld.org/
- United Nations High Commissioner for Refugees (UNHCR): http://www.unhcr.org/
- United Nations Office on Drugs and Crime (UNODC): http://www.unodc.org/
- UNDOC anti-trafficking : http://www.unodc.org/unodc/human-trafficking/

Non-governmental organizations (NGO)

- Human Rights Watch: http://www.hrw.org/
- Amnesty International: http: //www.amnesty.org/en/
- International Crisis Group: http://www.crisisgroup.org/
- World Organization Against Torture: http://www.omct.org/
- Anti-Money Laundering Forum: http://www.anti-moneylaundering.org/
- Open Society: http://www.opensocietyfoundations.org/

Think tanks

- United States Institute of Peace: http://www.usip.org/
- The Washington Institute: http://www.washingtoninstitute.org/
- Wilson Center: http://www.wilsoncenter.org/
- The MacKenzie Institute: http://www.mackenzieinstitute.com/
- Center for Strategic & International Studies: http://csis.org/index.php
- Council on Foreign Relations: http://www.cfr.org/
- Small Arms Survey: http://www.smallarmssurvey.org/
- Carnegie Endowment for International Peace: http://carnegieendowment.org/
- Brookings: http://www.brookings.edu/
- East-West Center: http://www.eastwestcenter.org/

- Critical Threats: http://www.criticalthreats.org/about
- International Institute for Counter-Terrorism: http://www.ict.org.il/
- Nuclear Threat Initiative: http://www.nti.org/

Research groups:

- Wisconsin Project on Nuclear arms control: http://www.wisconsinproject.org/
- South Asia Terrorism Portal: http://www.satp.org/
- Global Terrorism Database: http://www.start.umd.edu/gtd/
- The National Counter-Terrorism Center: http://www.nctc.gov/site/index.html
- Global Incident Map: http://www.globalincidentmap.com/
- Institute for the Study of Violent Groups: http://www.isvg.org/index.php
- Global Security: http://www.globalsecurity.org/index.html
- Protection Project: http://www.protectionproject.org/
- US National Security Archive: http://www.gwu.edu/~nsarchiv
- The Investigative Project on Terrorism: http://www.investigativeproject.org/about.php
- Combating Terrorism Center: http://www.ctc.usma.edu/publications/sentinel
- Human Security Gateway: http://www.humansecuritygateway.com
- Terrorist Organization Profiles: http://www.start.umd.edu/start/data_collections/tops

Interpol

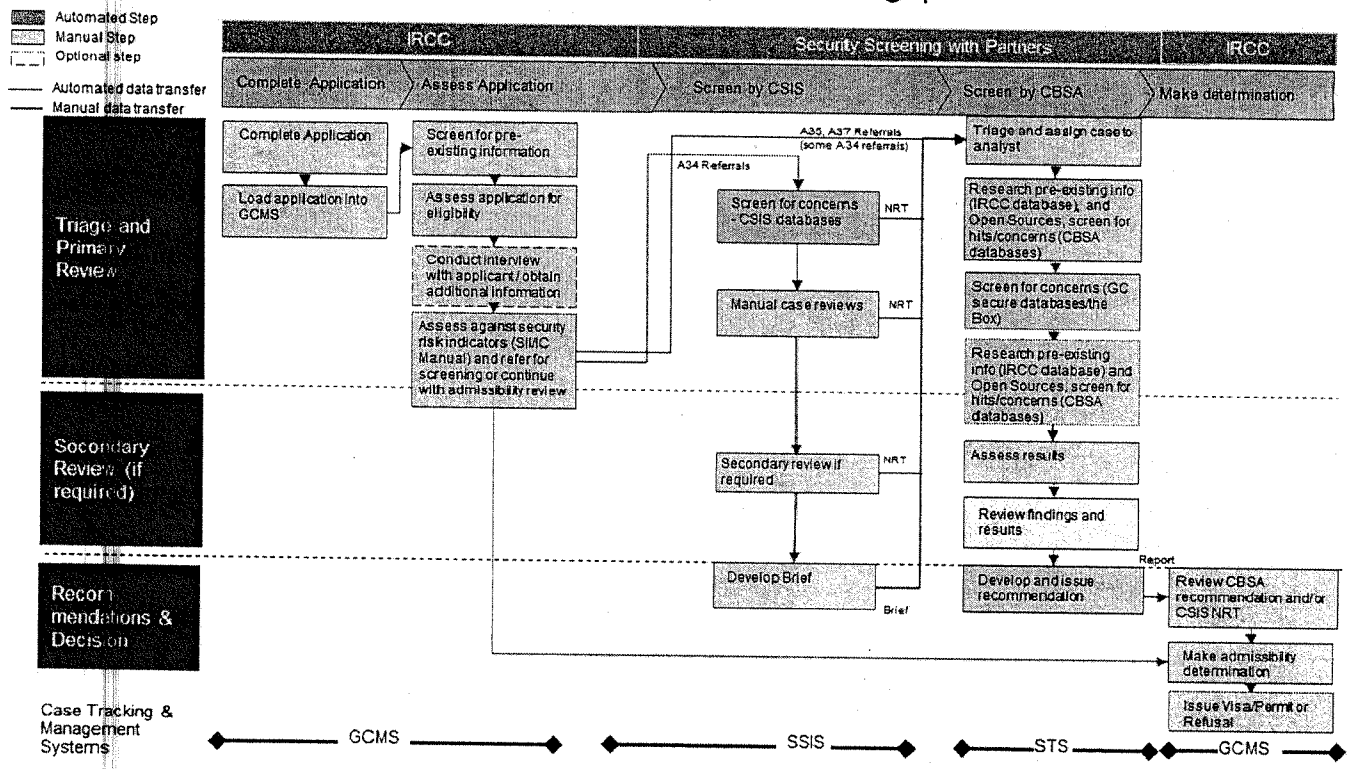
- Interpol Notices: http://www.interpol.int/INTERPOL-expertise/Notices

International Atomic Energy Agency

- https://www.iaea.org/

Appendix C:.

Overview of the security screening process



Appendix D: Sending Security Screening Requests for TR applications by email in the event of GCMS outage

1.1 **The following format is to be used for security screening requests (formerly VITs) originating from IRCC offices both within and outside of Canada.**

The information in bold is mandatory and must be included in the security screening request in the order in which it appears along with the appropriate answer. Security screening requests may not be processed if any of this information is missing which may result in delays.

Type of security screening request (VIT)	Email information
E-mail requests	• The title "Security Screening Request (VIT)" and subtype (A34, A35 and/or A37) • Mission • SURNAME (i.e. Smith) Example: VIT/A34/TEHRAN/SMITH If it is an urgent request, URGENT should preclude the above text in the example.

1. **Mission file # (V, S, W);**
2. **Name** (surname first in CAPITAL LETTERS and in parentheses, followed by given names); **provide aliases and any other names used by the applicant, including maiden names**;
3. **Date of birth (DD/MM/YY);**
4. **Gender;**
5. **Place of birth** (town and country) and details of when they left it (if applying from a different country);
6. **Home address**, e-mail address, home, work and cell phone numbers;
7. **Nationality** (if more than one citizenship, include them all);
8. **Passport number** (issued by – place of issue – date of issue – date of expiry);
9. **Current occupation – job title – name and address of employer**; (if student, should elaborate on institution, field and duration of study);
10. **Details of educational background and employment background;**
11. **Purpose/ function or position during visit to Canada;**
12. **Invited by: (persons, firms or organizations) all host contact information (home/business address, e-mail address, home, work and cell phone numbers). Indicate if there is a letter of invitation**;
13. **Previous travel** (officers should endeavour to provide as much detail as possible about itinerary and previous travel within the last 10 years, if available);
14. **Membership in any organization and positions occupied**;
15. **Service/contact with any police force, intelligence service, position held and responsibility;**

16. **Spouse's name (specify if accompanying or not), including maiden name if applicable followed by the given names and date of birth (DD/MM/YY);**
17. **Additional information to be added for someone having served in the military or with the police: they may be required to fill out the Military/Police Service Table**
18. **Existence of EII lookout on the applicant;**
19. Any additional comments.

19.1. Where to send a security screening requests (VITs) via email and who to copy

Security screening requests should always be sent via GCMS. However, in the event of a GCMS outage, requests should be sent as follows:

Concern	Addressee	Details
ALL VITs for section (s) 34, 35 and/or 37 of IRPA	1st Addressee NSSD	**REGARDLESS OF CONCERNS** The 1st addressee for security screening requests is the NSSD address.
VITs for section 34 of IRPA	2nd Addressee PILLAROTT	For VIT A34 cases PILLAROTT should be copied.
VITs for section 37 of IRPA	2nd Addressee RCMP	For VIT 37 cases, the RCMP should be copied for TR cases from Mexico only.
VITs sent to the NSSD **Also COPY**		If sensitive and/or potentially controversial high profile cases, as well as criminality concerns. (This copy is for info). Note this address also includes the current Director General and Senior Director of Case Management Branch and the Office of the Assistant Deputy Minister.
	IRCC International Region /Desk	If sensitive and/or potentially controversial high profile cases. (This copy is for info).

Note: If information for mandatory fields is missing from messages sent by email, the visa office will be asked to confirm the particulars of the missing information. The processing time will only commence when the requested information is received by the NSSD.

Appendix E: Basic areas to be explored during the interview

Part A - General Background

Preparing for an interview and using questionnaires

Officers conducting interviews to assess whether a foreign national is inadmissible to Canada pursuant to section(s) 34, 35 and/or 37 of IRPA should be prepared to conduct lengthy and in-depth interviews. Officers are encouraged to be well-prepared by conducting the necessary research in advance and by consulting with screening partners as required.

The following are suggestions on how to proceed:

- Review and scan all available information and intelligence and make sure the material used is relevant and credible. This may include: identification/travel documents; past travel; family background; education; occupation or career path; group membership or association with specific groups; business background (associates); funds and source of such funds; invitation letter; itinerary; and Canadian contacts.

- Prepare an interview plan according to the admissibility being addressed (see below). Contact the NSSD via for additional information and/or guidance.
  Depending on the answers received from applicants, officers may expand on the questions below.

During the interview

To prepare for an interview, officers should consult as much information and intelligence from a variety of sources as possible. While applicants should be asked direct and specific questions related to their past activities or involvement in groups, **officers should be cautious not to inadvertently reveal or discuss classified information or intelligence to the applicant during the interview**.

Part B - Inadmissibility

Statutory questions on application
According to section 16(1) of IRPA, a person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires.

Officers should be satisfied that all pertinent information has been included in the application and that all questions have been answered to their satisfaction. Below are examples of questions that may be asked during an interview, based on the type of admissibility being examined and listed under the relevant section(s) of IRPA.

A34(1) Security

A permanent resident or a foreign national is inadmissible on security grounds for:

- *(a) engaging in an act of espionage that is against Canada or that is contrary to Canada's interests ;*
- *(b) engaging in or instigating the subversion by force of any government;*
- *(b.1) engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada;*
- *(c) engaging in terrorism;*
- *(d) being a danger to the security of Canada;*
- *(e) engaging in acts of violence that would or might endanger the lives or safety of persons in Canada; or*
- *(f) being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c).*

For the purpose of 34(1)(f), Officers are encouraged to verify work and school historyand ensure applicants can account for the entire 10 year time period or longer if deemed necessary (PR applications only). The following questions are aimed at guiding the interview to determine if the applicant was/is a member of an organization or group engaged in acts of terrorism, espionage or subversion as described in A34(1)

Officers are encouraged to refer to the IC Indicator and related manual to assist their interview preparation.

A35(1) War crimes/crimes against humanity/genocide

A permanent resident or a foreign national is inadmissible on grounds of violating human or international rights for:

A35(1)(a)

committing an act outside Canada that constitutes an offence referred to in sections 4 to 7 of the Crimes Against Humanity and War Crimes Act;

If the applicant was a member of the military police, militia, or a rebel group, officers may consider the following questions:

A35(1)(b)

being a prescribed senior official in the service of a government that, in the opinion of the Minister, engages or has engaged in terrorism, systematic or gross human rights violations, or genocide, a war crime or a crime against humanity within the meaning of subsections 6(3) to (5) of the Crimes Against Humanity and War Crimes Act;

R16:

For the purposes of paragraph A35(1)(b) of the Act, a prescribed senior official in the service of a government is a person who, by virtue of the position they hold or held, is or was able to exert

significant influence on the exercise of government policy or is or was able to benefit from their position, and includes:

(a) heads of state or government;
(b) members of the cabinet or governing council;
(c) senior advisors to persons described in paragraph (a) or (b);
(d) senior members of the public service;
(e) senior members of the military and of the intelligence and internal security services;
(f) ambassadors and senior diplomatic officials; and
(g) members of the judiciary.

ENF 18, section 8.2 breaks down into three (3) categories persons who are inadmissible under section 35 (1)(b) of IRPA and lists the evidentiary requirements to establish inadmissibility for each category.

Category I:

- Named positions described in R16(a), R16(b), R16(f) ambassadors only, and R16(g);
- That a person is or was an official in this category is determinative of the allegation. Aside from the designation and proof that the person holds or held such a position, no further evidence is required to establish inadmissibility.

Category II:

- Senior positions described in R16(c), R16(d), R16(e), and R16(f) senior diplomatic officials

  In addition to the designation of the regime, the officer must established that the position the individual holds or held is indeed a senior one and should be related to the hierarchy in which the function operates. A general indicator is that an individual's position is positioned within the top half of the hierarchy of an organization.

Category III:

- Persons not described in R16;
- In addition to the designation of the regime, the officer must establish that the individual exercised significant influence on the action or policies of the regime or benefitted from the position.

The following questions may assist officers in determining if a position is described in R16(c): senior advisors to heads of state or government and or members of the cabinet or governing council; orR16 (d): senior members of the public service.

Appendix F – Who to contact at HQ

Issue	Who to contact	Email Address
For assistance in the context of security screening, officers should contact the NSSD	NSSD	
General assistance for section 34, 35 and 37 cases.	For section 34, 35 and 37 cases that do not fall within the purview of the NSSD (i.e. no screening request has or will be sent), officers may contact the Intelligence Operations and Analysis Division (IOAD) at the CBSA for general assistance in researching and/or obtaining additional information.	
Contentious, sensitive or high profile cases	**IRCC - Case Management Branch** manages contentious, sensitive and high profile cases on behalf of the Minister of Citizenship and Immigration. Case Management should be contacted and kept informed when officers become involved in such cases.	
	The **NSSD** should also be made aware of files when inadmissibility under sections 34, 35 and/or 37 of IRPA is involved.	
	CSIS should be made aware of cases involving national security issues related to section 34 of IRPA.	
General screening procedures	**IRCC**- Security, Admissibility and Screening Unit, Program Integrity Branch at IRCC HQ may be contacted by CPC-V or any overseas visa office: • for guidance on overall screening procedures; • for assistance or guidance on questions or issues related to security screening.	
Temporary Resident Permits (TRP) or PPTRV	Case Management Branch at IRCC should be made aware of files involving TRPs and PPTRVs.	

CBSA Border Operations Centre (BOC):
In case of an emergency outside of working hours, officers may contact the Border Operations Centre at (613) 960-6001 for consultation or discussion of cases related to section(s) 34, 35 or 37 of IRPA.

Canada Border Services Agency

Immigration Control Manual Chapter 2 (IC 2) - Security Screening Indicator Manual

Document Changes and Updates Tracking – December 31, 2016

Version 11 (2016)

Please Note: Duplication or further distribution of this chapter is not permitted without authorization from the Director, Intelligence, Targeting and Criminal Investigations Program Management Division, Enforcement and Intelligence Directorate, Programs Branch, CBSA.

December 31, 2016

Updates:

December 31, 2016

The Immigration Control (IC) Manual Chapter 1 – Security Screening of Permanent Residence Applications and the Immigration Control Manual (IC) Chapter 2 – Security Screening of Temporary Residence Applications, were restructured into an Immigration Control (IC 1) Manual and an Immigration Control (IC 2) Indicator Manual to reflect indicator led referrals for security screening.

This manual chapter contains the following information:

- general direction on how to use the screening indicators;
-
-
-

Table of Contents

1. What is this chapter about? 4
2. Security classification 4
3. Screening tools (indicator-led security screening) 5
3.1 The Security Integrity Index (SII) 5

7. General Indicators - Section 34(1) of IRPA .....
8. General Indicators - Section 35(1) of IRPA .....
9. General Indicators - Section 37(1) of IRPA .....
Annex A: Security Integrity Index (SII) 2015

1. What is this chapter about?

This manual chapter provides functional direction and guidance to officers on **when** to refer temporary resident (TR) or permanent resident (PR) applications and claims for refugee protection to the Canada Border Services Agency (CBSA) and screening partners for security screening for the following inadmissibility categories under the *Immigration and Refugee Protection Act* (IRPA):

- A34 - security (espionage, subversion, terrorism);
- A35 - War crimes, crimes against humanity and genocide; and
- A37 - Organized or transnational criminality.

Note: Instructions in this manual chapter should be read in conjunction with the Immigration Control Process Manual Chapter 1 (IC 1).

1.1. Streamlining the security screening referral process:

The information contained in this manual chapter provides for a streamlined security screening referral process for referring PR and TR applications.

Going forward, visa officers overseas and officers at CPC-O are to use all of the following tools to determine when to refer temporary or permanent resident applications for security screening.

- indicators[1] (listed in section 5 of this manua)l;
- General indicators[2] listed in Section 6, 7, and 8 of this manual; and
- The Security Integrity Index (SII)[3], prepared by CSIS, located in Annex A of this manual.

Note:

2. Security classification

This manual chapter (IC Indicator manual) is classified at the secret level because it contains sensitive information that if released could cause injury to the national security of Canada.

Information contained in this manual is intended for Immigration, Refugees and Citizenship Canada (IRCC) and CBSA officers who are involved in the security screening process, and who

[1] Previously used to screen temporary resident applications only.
[2] Previously used to screen temporary resident applications only.
[3] Previously used to screen permanent resident applications only.

have the appropriate security clearance and 'need to know' the information. **Under no circumstances shall this manual be made available to locally engaged staff (LES) at visa offices overseas.**

Note: As per the *Policy on Government Security*, the IC 2 manual must be stored in approved containers.
For additional information on classification of information in the context of security screening, please refer to the IC Process Manual.

3. Screening tools (indicator-led security screening)

3.1 The Security Integrity Index (SII) (Annex A)

The SII is developed and maintained by CSIS and includes screening indicators that are intended to assist officers in determining which applications should be referred to CSIS for security screening.

- Officers should screen all against the screening indicators based on the instructions provided in the SII.

3.2 screening indicators

screening indicators (section 5 of this manual chapter) were developed by the to assist officers in identifying individuals who may be inadmissible to Canada pursuant to section(s) 34, 35 and/or 37 of IRPA. ndicators consist of mandatory and discretionary indicators.

1. Mandatory screening indicators

Mandatory screening indicators are meant to flag who may pose a high risk to the safety and security of Canada. that meet one or several mandatory indicator **must** be referred for security screening as per the instructions in the IC 1 (Process Manual).

Examples include, but are not limited to the following:

- from foreign nationals who are subject to a lookout (Enforcement Information Index (EII),
- from foreign nationals who were members and/or supporters of an organization or group that is listed as a mandatory referral.

2. Discretionary screening indicators

Discretionary screening indicators are meant to provide guidance to officers on making referral decisions. If a discretionary indicator is met, officers should continue to review the application

in its entirety to determine if admissibility concerns pursuant to section 34, 35 and/or 37 exist, in which case the application should be referred for security screening; unless the officer has sufficient information to render the individual inadmisible..

Note:

Examples include, but are not limited to the following scenarios:

3.3

- section 6 of this manual chapter for s. 34 of IRPA;
- section 7 of this manual chapter for s. 35 of IRPA; and,
- section 8 of this manual chapter for s. 37 of IRPA.

General screening indicators consist of mandatory and discretionary indicators. Please refer to section 3.2 above for examples on how to apply mandatory and discretionary screening indicators.

Note: pursuant to section(s) 34, 35 and/or 37, the decision maker should refuse the application without sending it for security screening

nder sections 34, 35 and/or 37 as outlined in section 18.1 of the IC1 Process Manual.

Annex A

SECURITY INTEGRITY INDEX (SII) 2015

December 31, 2016

To CIC,

You will find below the 2015 version of the Security Integrity Index (SII) which provides national security indicators for use by CIC Immigration Program Managers (IPM) and other CIC Canada-based staff to assist in determining should be referred to CSIS for security screening in accordance with both *the Immigration and Refugee Protection Act* (IRPA) and the *Canadian Security Intelligence Service Act* (CSIS Act).

You will notice that this present iteration of the SII places a greater emphasis on based upon concerns which relate to threats to the security of Canada. The Service considers that this revised tool will greatly assist CIC in streamlining referrals and will support a more concise review process.

CSIS remains committed to focusing our efforts on national security threats as defined in the CSIS Act and, therefore we anticipate that our partners will continue to render admissibility decisions based upon information at their disposal, in addition to referring relevant cases to CSIS.

Should you have any questions or require any assistance in interpreting the revised SII, please do not hesitate to contact us,

Best regards,

Director General
Security Screening Branch
Canadian Security Intelligence Service

SECURITY INTEGRITY INDEX (SII)

This reference document is classified SECRET - Canadian Eyes Only

It is prepared by the Canadian Security Intelligence Service (CSIS) Security Screening Branch for the express use of Citizenship and Immigration Canada (CIC) Immigration Program Managers (IPMs), CIC Canada – based staff and CSIS Foreign Collection Officers (FCOs). This document is not to be further disseminated, in whole or in part, without written permission of the CSIS Executive Director General, Security Screening.

Kindly direct any comments / suggestions regarding changes to the format or updating of the SII to CSIS Security Screening Branch or via telephone at

I. OVERVIEW

Article I. 1) OVERSEAS SECURITY SCREENING GUIDELINES

INTRODUCTION

The role of CSIS is to provide security advice in accordance with Section 14 of the *CSIS Act*, to the Canada Border Services Agency (CBSA) and CIC. This security advice relates the threats to the security of Canada as defined in Section 2 of the *CSIS Act* and is provided to assist CIC and CBSA in the exercise of their duties and functions in accordance with the *Immigration and Refugee Protection Act* (*IRPA*), particularly as it relates to the inadmissibility provisions listed in Section 34 (1). The decision to refuse admissibility to Canada on security or other grounds of the IRPA rests with CIC. It is important to note that CSIS does not provide advice with respect to an individual's inadmissibility to Canada.

FUNCTION OF THE SII

The SII provides national security indicators for use by IPMs and other CIC Canada-based staff to assist in determining should be referred to CSIS for security screening. The SII is also used to provide functional guidance to CSIS Foreign Collection Officers (FCOs) with respect to their role in the security screening process.

STRUCTURE OF THE SII

The SII is divided into four (4) sections:

-
-
-
-

Every must be compared against all four sections to ensure that all national security concerns are addressed.

2) OVERSEAS PERMANENT RESIDENT SCREENING PROCESS

The following business process must be applied in the review of overseas applications.