Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

TOP SECRET

File No.: 2800-161
(TD R513)

CSIS'S ROLE IN THE SECURITY CERTIFICATE PROCESS

(SIRC STUDY 2011-02)

Security Intelligence Review Committee
December 5, 2011

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

TABLE OF CONTENTS

1 INTRODUCTION 2

2 METHODOLOGY 4

3 SELECTED ISSUES IDENTIFIED IN THE SECURITY CERTIFICATE PROCEEDINGS 5

3.1 Duties of Good Faith and Candour 6
3.2 Witness Preparation 6
3.3 Meeting the Legal Standard 7

4 CSIS'S RESPONSE 9

4.1 Human Source Précis 9
4.2 Preparing Witnesses 10
4.3 Training and Awareness Building 11

5 ISSUES FOR CONSIDERATION 13

5.1 Use of SIRs in Immigration Proceedings 13
5.1.1 Need for Clarity 15
5.1.2 IAB Engagement 16
5.2 Strategic Approach 16

6 CONCLUSION 19

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

1 INTRODUCTION

A security certificate is a legal tool that allows the Canadian government to detain and to deport non-Canadians (permanent residents or foreign nationals) deemed to be security threats. The security certificate process is set out in the *Immigration and Refugee Protection Act (IRPA)*; it is an immigration, not a criminal, proceeding. Certificates can be issued on grounds of security, which include espionage and terrorism, as well as for violating human and international rights, serious or organized criminality.

CSIS's principal role in the security certificate process is to prepare a Security Intelligence Report (SIR), a document containing its information and assessment that an individual poses a threat to national security.[1] The CSIS Director himself reviews and approves all SIRs that are prepared by Litigation Branch; the document is then forwarded to the Ministers of Public Safety and Citizenship and Immigration for their approval.[2] The Ministers file a Notice of Referral of Certificate together with the SIR and supporting reference materials with the Federal Court, where a judge must make a determination on the "reasonableness" of the certificate. Although security certificates have existed since 1978, they have seldom been used.

The federal government has used certificates as a counter-terrorism tool, issuing certificates against five men suspected of ties to terrorism. In recent years, the regime has become, and is still, heavily litigated. The outcome has been numerous rulings from the Federal Court and a major decision in 2007 from the Supreme Court of Canada in *Charkaoui v. Canada*[3], which struck down the certificate regime as unconstitutional and forced a reform that provided for the appointment of special advocates to represent the interests of the named persons during the closed security certificate proceedings. In the context of these legal challenges, the advice CSIS provided to the Ministers of Public Safety and Citizenship and Immigration has also come under heavy scrutiny.

As part of SIRC's examination of the challenges posed by the increased use of CSIS intelligence in legal proceedings, the purpose of this review is to examine the Service's internal processes and policies related to its role in the security certificate process and

---

1 There are two versions of the SIR - the public summary and the classified version.

2 In addition to preparing the SIR, CSIS may also testify at reasonableness hearings, detention reviews, and other Court proceedings in relation to security certificate cases.

3 *Charkaoui v Canada (Citizenship and Immigration)* [2007] 1 SCR 350 [*Charkaoui No. 1*]

ATIP version
MAR 14 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

how these have changed to accommodate a number of issues raised in the context of security certificate proceedings. This includes the Service's current thinking on the security certificate process, and CSIS's role in this broader whole-of-government discussion.

In several important respects, CSIS has taken steps to respond to the issues that have been raised in these proceedings, especially as they relate to providing information on human sources to the Court; preparing Service witnesses who appear before the Court; and implementing training initiatives to instill in CSIS employees an appreciation of the need for on-going attention to rigour in all activities. The Service has also created the Litigation Committee and the Litigation Branch, which houses civil and immigration litigation under one roof in the hopes of building expertise and fostering consistency in all aspects of Service litigation.

At the same time, SIRC believes that it may be time for CSIS to undertake a more holistic examination of the issues and criticisms emanating from the substantial corpus of judicial rulings, in order to assess their cumulative impact on CSIS processes and practices. To this end, SIRC recommends that CSIS take a more strategic approach to managing the challenges associated with the use of intelligence in legal proceedings.

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

2 METHODOLOGY

The objective of this review was to examine CSIS's response to some of the issues identified by the Federal Court in two of the recent security certificate cases - Mohamed Harkat and Hassan Almrei[4] - and consider how they challenged the Service to look critically at its involvement in security certificates, such as: the process and substance of human source information provided to the courts; the guidelines related to the Service documents prepared in support of security certificates; the preparation of witnesses appearing before the Court; and, more generally, its practices with respect to the presentation of intelligence in legal proceedings.

In addition to a review of CSIS documentation, SIRC staff attended several briefings with CSIS personnel involved in different aspects of the security certificate process, including staff from the
Litigation Case Management unit. Although documents pertaining to government-wide discussions on developing an alternatives to removal were subject to Cabinet confidentiality, SIRC was given summary information on the form and substance of these discussions orally.

[4] Hassan Almrei is a Syrian national who entered Canada in 1999 and was granted refugee protection. He was named in a security certificate in 2001 and was detained for approximately eight years before being released with conditions. His certificate was quashed in 2009. Mohamed Harkat, an Algerian refugee claimant, was detained under a security certificate in 2002 and released from detention with conditions in 2006. In 2010, his certificate was upheld as reasonable and a deportation order against him was issued; he is appealing that decision. The other three certificates that will not be examined are against Mahmoud Jaballah, Mohamed Mahjoub and Adil Charkaoui. The Charkaoui certificate, which is notable for being associated with the Supreme Court of Canada decision that found the certificate system unconstitutional, was quashed. The remaining two certificates, against Mahmoud Jaballah and Mohamed Mahjoub, are still being adjudicated.

ATIP version
dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3 SELECTED ISSUES IDENTIFIED IN THE SECURITY CERTIFICATE PROCEEDINGS

In recent years, the five individuals subject to certificates for suspected ties to terrorism have launched multiple legal challenges. Among the most noteworthy rulings is the 2007 Supreme Court of Canada ruling in the Charkaoui case, which found elements of the security certificate system in violation of the *Charter*.[5] In response, the government amended *IRPA* to include provisions for "special advocates" - security cleared lawyers who are there to represent the interests of the named person in closed-door court hearings in which the judge assesses the "reasonableness" of the certificate[6], and by extension, the validity of CSIS's information, all without the presence of the named person or his or her lawyer.[7] The scrutiny of these special advocates has brought to light several issues pertaining to CSIS's involvement in the certificate process.[8]

This section focuses on three key issues that emerged in the context of the security certificate proceedings related to Harkat and Almrei, namely - the Service's duties of good faith and candour; the preparation of witnesses; and the challenge of meeting the legal standard in security certificate cases. These issues were significant as they not only called into question CSIS's credibility before the Court, but more importantly, compelled CSIS to examine how it presents intelligence before the courts.

---

5 The second Supreme Court of Canada ruling in Charkaoui in 2008 is significant because it required CSIS to change its policy and practices on information retention. CSIS must now retain originals of its information in most situations. The case requires the Service to disclose the named person's entire file to the special advocates; this information is then vetted for national security privilege and released (usually in summary form) to the named person. This is an important development that would require its own review; as such, it will not be treated here.

6 The special advocates also represent the interests of the named person in detention reviews and pretrial hearings.

7 Following the changes to *IRPA*, the five terrorism related security certificates effectively lost their status and new security certificates were issued, which required CSIS to redraft the SIRs. In February 2008, the Ministers signed the five new certificates and the amended SIRs were filed with the Federal Court, which was again asked to rule on the "reasonableness" of the certificates.

8 In December 2010, the Federal Court ruled that the Harkat certificate was reasonable and ordered his deportation. This ruling marked a substantial victory for the government because the judge found that the security certificate alleging Harkat is a terrorist threat was reasonable; CSIS's investigative missteps did not constitute "abuses" significant enough to fundamentally undermine the Harkat case; and third, the government's security certificate powers were consistent with the *Canadian Charter of Rights and Freedoms*. The Harkat decision is currently being appealed.

ATIP version
MAR 14 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

3.1 Duties of Good Faith and Candour

In an October 2009 decision on the Harkat certificate, a Federal Court judge noted that "the failure of CSIS, and of its witnesses, to act in accordance with the obligation of utmost good faith...has undermined the integrity of this Court's process".[9] The judge arrived at this conclusion after learning that CSIS had failed to disclose that one of the key sources used in the case had failed a polygraph test. To its credit, the Service brought this issue to the Court's attention, but not until months after the judge had specifically asked CSIS witnesses about the source's reliability. In the *ex parte* session following CSIS's disclosure, the judge was explicit that although CSIS might have its own opinion as to the reliability of a human source, "when the judicial process is on [...] CSIS has no right to take away information that permits me to make up my own mind as to the reliability of a source".[10]

Similarly, in a ruling in the Almrei case, the Federal Court judge found that CSIS and the Ministers were "in breach of their duty of candour to the Court" by not having conducted a thorough review of CSIS's information holdings on Almrei and by not having made representations based on all of the information, including that which was unfavourable to their case. The judge found that CSIS's Security Intelligence Report (SIR) "was assembled with information that could only be construed as unfavourable to Almrei without any serious attempt to include information to the contrary."[11] At issue was the judge's belief that CSIS had withheld information, and therefore failed to present complete information to the Court.

3.2 Witness Preparation

In part, one of the issues raised by the judge in the Harkat case was rooted in how CSIS prepared its witnesses before appearing in Court. In his ruling, the judge noted that a CSIS witness was given several opportunities during his testimony "to disclose the polygraph information, and he did not do so. His explanation that 'it was not in mind' is not satisfactory".[12] He was also critical of two other CSIS witnesses, whom he found were inadequately prepared and gave incomplete information to the Court.

---

9 *Harkat (Re)* 2009 FC 1050 at para 59.

11 *Almrei (Re)* 2009 FC 1263 at paras 503 and 500.

12 *Harkat (Re)* 2009 FC 1050 at para 27.

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In a letter to the Federal Court, the Senior General Counsel for CSIS acknowledged that the non-disclosure of the polygraph information raised questions regarding the "possible prevarication of CSIS witnesses called to testify concerning the reliability of the information provided by the human source."[13] In the end, the judge concluded that the witnesses did not intend to deceive the Court, nor should they "bear all the blame for what appears to be [...], in part, an institutional failure of CSIS." Still, he believed the situation to be "unacceptable" since, as an institution, "CSIS must ensure that the witnesses they call to testify are properly educated about the function they are being asked to undertake; they must be thoroughly prepared by legal counsel".[14]

3.3 Meeting the Legal Standard

In addition to his finding that CSIS had failed in its duty of candour before the Court, the presiding judge in the Almrei case also found that CSIS had relied on outdated information and poorly-substantiated allegations in order to maintain the certificate against him. He therefore concluded that the information and evidence did not satisfy the threshold of "reasonable grounds to believe" as required by *IRPA*.

The judge found that information provided by CSIS human sources who were instrumental in upholding the case against Almrei was not credible, in part because of intercept and surveillance reports that contradicted human source reporting.

The ruling called attention to some of the inherent difficulties in using human source information in judicial proceedings, especially given the absence of written records and the judge's belief that much human source reporting amounts to "hearsay upon hearsay". Although this type of information may be used in certificate cases, the Court must determine if the information is "reliable and appropriate".[17] In many instances, the

13 *Harkat (Re)* 2009 FC 553 at para 12.

14 *Harkat (Re)* 2009 FC 1050 at paras 44-45.

17 *Almrei (Re)* 2009 FC 1263 at para 83.

ATIP version dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

judge found that the information provided by CSIS was not,

ATIP version
dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

4 CSIS'S RESPONSE

The Service responded to the Court's concerns in a number of ways. First, it developed policy to govern the preparation and approval of the human source précis, an important document that CSIS uses to convey information on human sources to the Court. Additionally, a number of concrete steps were taken to improve the process of preparing witnesses for testimony in security certificate cases. Finally, CSIS developed an extensive training program focused on promoting "rigour" in all activities.

Although the Service did take steps to address the specific concerns raised in these cases, as will be discussed in the next section, SIRC believes that the Service could be more strategic in its approach to managing its engagement in legal processes.

4.1 Human Source Précis

CSIS recognized the gravity of its failure to disclose in a timely manner important human source information to the judge in the Harkat certificate. In a letter to the Chief Justice of the Federal Court, the CSIS Senior General Counsel wrote that, insofar as the situation gave the Court any cause to question the integrity of CSIS's evidence and of its employees, the Service was "resolute in its determination to restore judicial confidence in that integrity and credibility".[19] To that end, CSIS quickly undertook a complete review of all security certificate human source précis to ensure that no other information had similarly been withheld from the Court. précis were reviewed and amended.[20]

The Service also promptly initiated a thorough managerial review of the procedures surrounding the preparation of human source précis. The review concluded that the "lack of centralized control and coordination over source précis led to inconsistencies in both format and content, and could impact on its capacity to meet requirements for full, fair and frank disclosure as they apply in relation to assessments of the reliability and credibility of the Service's human sources and their information".[21] As a result, procedures for the preparation of source précis were formalized in a policy requiring all such précis to be prepared in consultation with Legal Services, and to be reviewed

Each précis is also now submitted to a challenge session (in which counsel participates) in order to review, and ensure the accuracy of, each statement in

---

19 Letter from CSIS Senior General Counsel to the Honourable Allan Lutfy (June 4, 2009).

20 The result was the detection of errors, mostly minor, source files reviewed. July 12 briefing

21 Letter from CSIS Senior General Counsel to the Honourable Allan Lutfy (May 20, 2010).

ATIP version
dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

the document. Moreover, the policy outlines the kind of information to include in the précis, information which the Court needs to make an independent assessment of the reliability of a human source. To complement the policy, a guideline document was developed to communicate further the kind of information that should be given special mention in the précis.

SIRC found that CSIS appreciated the significance of the Court's finding and took action, first to determine the cause of the mistake, and second, to put in place corrective measures to avoid a reoccurrence. Given that human source précis are also used to support warrant applications, this new policy has a broad application.

4.2 Preparing Witnesses

The managerial review also explored how CSIS prepared its witnesses in light of the judge's suggestion of possible witness prevarication.[22] One of the key observations of the managerial report was that there were no guidelines for Service witnesses appearing before the courts in security certificate cases.

SIRC was told that CSIS's Departmental of Legal Services (DLS), which are functionally part of the Department of Justice (DoJ), and which is responsible for witness preparation, has prepared a guide for witness preparation that covers issues specific to security certificates. As much as possible, counsel are encouraged to spend all the time required to prepare witnesses and to ensure that "...the witness understands the consequences of giving misleading or inaccurate information (whether inadvertently or deliberately) to the Court."[23] CSIS's Litigation Case Management Units (LCMU) play a supportive role by coordinating and collecting relevant documents for the witness to review, obtaining prior Service testimony on similar issues and other background documents as required, and assisting DLS in selecting witnesses.

SIRC found that steps have been taken to equip Service employees testifying in security certificate cases. This is especially important given that CSIS employees must now testify in Court in the presence of special advocates, which has been described as an important "new reality."[24]

Additionally, the policy on human source précis

---

22 *Harkat (Re)* 2009 FC 553 at para 12.

23 Service memo prepared in response to SIRC questions of July 22, 2011.

24 *Harkat (Re)* 2009 FC 1050 at para 50.

ATIP version
dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

This addresses a serious concern of the judge in this case, that legal counsel was not given access to sufficient factual information on which to base important legal advice.[26]

4.3 Training and Awareness Building

In his Directional Statement for 2009, the Deputy Director of Operations (DDO) emphasized the concept of "rigour" as a CSIS corporate standard in order to "draw attention to this [rigour] as an individual and organizational priority."[27] To this end, Training and Development Branch was given responsibility for putting in place a 'cradle to grave' program training as it relates to rigour.[28]

SIRC was given information on the extensive activities that have been developed to promote the concept of rigour within CSIS, including high level statements stressing the need for rigour across the organization. SIRC was also advised that the importance of rigour, and the consequences for CSIS of not being rigourous, are reinforced throughout the Intelligence Officer Training Course (IOTC). Additionally, DLS has developed a "judicial orientation module" given to new intelligence officers covering a broad range of legal topics and issues, including, *inter alia*: intelligence to evidence; disclosure; giving testimony; and the *Charter*. Legal training provided by DLS is also available to current employees as appropriate/required. Finally, gives presentations to CSIS regional staff on issues that have been identified in the courts and their practical implications.

---

26 *Harkat (Re)* 2009 FC 1050 at paras 44 and 45.

27 DDO Directional Statement for 2009

28 A useful definition of rigour specific to intelligence work has been developed and disseminated throughout the Service: "A disciplined approach to carrying out day-to-day business that stresses: attention to detail; accuracy and verification of facts; thoroughness, and; balanced objectivity in assessing threats and reporting information. Lapses in rigour may not become evident for years and may end up having serious consequences for the Service in terms of our reputation, credibility, and relationships with important domestic institutions such as the Federal Court. Operational reports form the basis of many of the intelligence products the Service creates and the advice we give to government. Selectivity, omission, superficiality, conjecture and spin are toxic to the intelligence production continuum and must never be allowed to seep into the process, degrade the quality of our work and ultimately debase the advice we give to government."

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

SIRC was satisfied that the Service is using training and awareness activities at different levels and in innovative ways to inculcate in its employees a sensitivity to, and awareness of, the need for "rigour".

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

5 ISSUES FOR CONSIDERATION

CSIS faces substantial disclosure obligations with the security certificate process and, because some of the intelligence used in SIRs comes from foreign agencies, disclosure can be especially problematic. There are discussions currently taking place within government on developing alternatives to removal;[29]

5.1 Use of SIRs in Immigration Proceedings

CSIS continues to fulfill its duties to investigate foreign nationals and permanent residents who are threats to national security, and to provide advice to the

[29] These discussions have been on-going since at least 2003. Since 2009, CSIS has participated in an Alternatives to Removal Working Group (ATRWG) that was created to explore options.

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Minister.[32] As a result, CSIS will remain involved in immigration proceedings, such as in *IRPA* section 86 proceedings, which allow the Minister to apply for the non-disclosure of information or other evidence during admissibility hearings, detention reviews or appeals before the Immigration Appeal Division. In these proceedings, like the security certificates, CSIS must prepare a SIR that can be challenged by special advocates.[33] Of note, CSIS was advised that it should "provide the classified information in a section 86 case in the same manner and with the same rigour that is applied in the security certificate cases." There were suggestions in the document review that the national security-related cases under the section 86 process represents a potential "next phase" in immigration cases, Moreover, Public Safety has indicated that, as of 2010, there were three active section 86 "cases".[36] In short, when CSIS secret intelligence underpins a section 86 proceeding, it will have to prepare a SIR.

CSIS has indicated that should it "enter into a new security certificate proceeding in the future (and draft a corresponding SIR), Litigation Branch would look to lessons learned in all of the security certificate cases to ensure that any document prepared is done with

32 The Service has the sole responsibility for screening immigrants and refugees who apply for permanent residence status from within Canada.

33 The main procedural difference between section 86 proceedings and security certificates is that, where the reasonableness of the certificates is determined by a judge of the Federal Court, section 86 proceedings are adjudicated by the Immigration and Refugee Board (IRB).

36 "Final Report, *2009-2010 Evaluation of the Security Certificate Initiative*, Public Safety Canada. Http://www.publicsafety.gc.ca/abt/dpr/aval/_fsi-ics-09-10-eng.pdf , p. vi.

ATIP version
MAR 1 4 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

the utmost attention paid to rigour, detail and candour."[37] However, in light of CSIS's ongoing involvement in section 86 proceedings, SIRC believes that it should re-consider implementing the recommendation made in the managerial review with respect to the preparation of SIRs. Furthermore, insofar as the information provided by CSIS on applicants for permanent residency may also be examined and challenged, it might be worthwhile for CSIS to examine whether the Court's observations in security certificate cases also apply to the classified briefs it provides to support a finding of inadmissibility.

5.1.1 Need for Clarity

SIRC has seen multiple statements reflecting CSIS's awareness of, and commitment to, its duty of good faith and candour before the courts. This position is reflected in the *Guidelines on Disclosure Obligation in Security Certificate Cases* that state "there has been a move to the disclosure of all relevant information. As enunciated in the case law, the information or evidence presented must be complete and thorough,

of information, leaving it to the Court to determine the value of the additional pieces of information."

Yet, there appears to be lingering ambiguity with respect to CSIS's duty to the Court when preparing a SIR. In particular, the judge in the Almrei case pointed out that "the Ministers stated that the SIR [...] is merely a document crafted by CSIS to plead their case and does not need to present the contradictory information within their possession." But in the judge's view, that position "is clearly incompatible with the duties of good faith and candour which the Court expects from the Service and the Ministers." Accordingly, he found that CSIS and the Ministers were "in breach of their duty of candour to the Court".[39] SIRC encourages CSIS to ensure that any ambiguity over its duties before the Court should be resolved as soon as possible.

---

37 Service memo prepared in response to SIRC questions of July 22, 2011.

39 *Almrei (Re)* 2009 FC 1263 at para 509.

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

5.1.2 IAB Engagement

Finally, SIRC believes there is merit in engaging the Intelligence Assessment Branch (IAB) in any future SIR preparation process. This consideration is driven by criticism emanating from the Almrei case in which the judge stated that "[a] great deal of knowledge has been acquired since 2001 about Al Qaeda's methods of operation" that was not reflected in the SIR, much of which would not have supported the premise that Almrei was a sleeper agent. The judge found it "troubling" that the work done by CSIS to prepare the SIR "had not kept pace with developments in the field. And the sources relied upon by the Service were often non-authoritative, misleading or inaccurate".[41]

In 2006, the IAB was created and positioned at the "centre" of the intelligence cycle. In light of IAB's analytical capacity, SIRC would encourage this Branch to be involved in the SIR preparation process. This approach would be consistent with a previous recommendation made in the 2008 DDO *Review of Warrant Acquisition Process* that IAB be involved in the drafting and maintaining of case briefs used in the warrant application process.

5.2 Strategic Approach

In response to it being drawn increasingly into the world of courts and evidence, CSIS has expressed its commitment to continue "to study the difficulties in presenting intelligence as evidence within the Canadian legal framework." It is also working "diligently to attempt to anticipate and address these issues to enable a more seamless use of intelligence in legal proceedings."[42]

This review underscored the importance of CSIS stepping up to this challenge, and adapting as quickly as possible its practices in response to observations and findings of the courts. The human source information to be provided in legal proceedings is a case in point: in 2005, one of the judges involved in the Harkat case provided a detailed list of "relevant inquiries and areas for examination"[43] concerning the information needed by

[41] *Almrei (Re)* 2009 FC 1263 at paras 358, 425, 413.

[42] Service memo prepared in response to SIRC questions of July 22, 2011.

[43] It is also noteworthy that the judge referred specifically to this list in his decision that followed the admission by CSIS that it had not disclosed the polygraph information.

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

the Court to undertake an independent review of the reliability of human sources;[44] however, much of this information was still missing from the information filed with the Court three years later. In fact, CSIS did not take action to develop the policy on human source précis until after the serious situation created by the omission of the polygraph information. It is worth noting that the list identified by the judge in 2005 is included, almost verbatim, in that new policy.

At the same time, there are other issues emerging from recent rulings that may warrant examination or action by the Service.

The judge in the Toronto 18 case indicated that the application of the third-party rule represents "an emerging area of importance in the Federal Court jurisprudence."[45]

More generally, since the threshold set out in *IRPA* of "reasonable grounds to believe" is qualitatively different from section 12 investigations that require "reasonable grounds to suspect", it may be necessary for the Service to adapt its methods of analysis and assessment to meet this legal requirement.

Thus, before providing advice on immigration cases that are subject to judicial or quasi-judicial challenge, SIRC suggests that the Service may consider taking steps to educate its staff on what this threshold means and how it is distinguished from "reasonable grounds to suspect".

SIRC has seen internal exchanges within CSIS senior management describing the Service's current approach to responding to court rulings as "piecemeal" and advocating the need to develop a more "global strategy" to ensure that it meets the standards required of it by the courts.[47] In light of these observations, and SIRC's own belief that the courts are providing important direction to the Service on the manner in

44 *Harkat (Re)* 2005 FC 393 at para 94.

45 R. V. Ahmad, Ruling No. 16 (2009-07-06) Brampton CRIMJ(F)2025/07 (Ont. S.CJ) at para 46.

47 document - Note de Service Advisory Letters.eml

ATIP version
dated: MAR 14 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

which it must carry out its duties to meet legal challenges successfully, **SIRC recommends that CSIS undertake a comprehensive and forward-looking review of relevant court rulings to ensure a full understanding of their implications on Service operations, processes and resources.**

ATIP version
dated: MAR 1 4 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

6 CONCLUSION

Adapting to the new disclosure requirements associated with security certificates and the presence of special advocates has been a legitimate challenge for the Service, This is the inevitable consequence of working in a fluid legal environment.

The experience with security certificates in anti-terrorism cases has raised significant questions concerning their effectiveness as a national security, and even immigration, tool. There is wide speculation that the increasingly complex legal environment may compel the government to stay away from certificates in the future.[48]

At the same time, there will continue to be a need for a process to deport from Canada permanent residents or foreign nationals who are determined to be inadmissible on national security grounds. This is reflected in a Public Safety Canada internal audit report which notes that, despite the complexities involved in balancing individual rights with the protection of national security, "there is a continuing need to litigate SC [security certificate] cases through the Federal Courts; there are pending *IRPA* section 86 cases; and there is a continuing need to process applications for permanent residency using classified information."[49] As a consequence, there is a continuing need for CSIS to make efforts to meet the challenges associated with the presentation of classified information in legal proceedings, both criminal and immigration.

[48] "Special advocates predict no more security certificates", *The Lawyers Weekly* (July 16, 2010).

[49] 2009-2010 *Evaluation of the Security Certificate Initiative*, Public Safety Canada.

ATIP version
MAR 1 4 2019
dated: