Our file: 117-2004-76

February 25, 2005

Nathan J. Whitling
Parlee McLaws, LLP
Barristers & Solicitors
1500 Manulife Place
10180-101 Street
Edmonton, Alberta
T5J 4K1

Dear Mr. Whitling:

This refers to your Access to Information Act request of January 19, 2005, for policy and procedures concerning the conduct of interviews of individuals and policy and procedures concerning note taking and statements given to individuals concerning their rights as interviewees, received on January 26, 2005. A receipt for your $5.00 application fee is attached.

Enclosed please find a copy of the releasable material pertaining to the subject of your request. Portions of the material have been exempted from disclosure by virtue of section 15(1) (as it relates to the efforts of Canada towards detecting, preventing or suppressing subversive or hostile activities) of the Act.

Should you wish to obtain clarification concerning your request, please use the information at the bottom of this letter to either call or write us. Please provide the file number at the top of this letter for reference purposes.

You are entitled to register a complaint with the Information Commissioner concerning your request. If you wish to exercise this right, notice of complaint should be addressed to:
Information Commissioner, Tower “B”, Place de Ville, 112 Kent Street, Ottawa, Ontario, K1A 1H3.

Yours truly,

Nicole J. Albert
A/Coordinator
Access to Information and Privacy

Attachments

P.O. Box 9732, Station “T”, Ottawa, Ontario K1G 4G4  C.P. 9732, Succursale “T”, Ottawa (Ontario) K1G 4G4
OPS-201 CONDUCT OF OPERATIONS - GENERAL

1. INTRODUCTION

Policy Objective

1.1 The objective of this policy is to provide direction on the conduct of operations by the Service as mandated by the CSIS Act and in accordance with Ministerial direction.

Scope

1.2 This policy outlines principles and standards for conducting Service operations.

1.2.1 For specific guidelines pertaining to contact with representatives of fundamental institutions of our society, see OPS-202, "Conduct of Operations - Fundamental Institutions of Society".

Authorities

1.3 CSIS Act

1.4 Ministerial Direction on CSIS Operations

References

1.5 OPS-100 to OPS-105, "Targeting - Section 12 CSIS Act"

1.6 OPS-601 to OPS-603, "Authorized Disclosure of Operational Information and Intelligence"

1.7 OPS-204 to OPS-208, "Human Sources"

1.8 OPS-217, "Operational Notes"

1.9 OPS-210, "Execution of a Warrant"

1.10 HUM-205, "Breaches of Conduct and Discipline"


Definitions

1.12 For reference purposes, definitions of fundamental terms have been provided in Appendix I.

2. PRINCIPLES

2.1 All CSIS operations will be governed by the following principles:
i) the rule of law must be observed.

ii) the investigative means must be proportional to the gravity and imminence of the threat.

iii) the need to use intrusive investigative techniques must be weighed against possible damage to civil liberties or to fundamental social institutions.

iv) the more intrusive the investigative technique, the higher the authority required to approve its use.

v) the least intrusive investigative methods must be used first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat.

3. STANDARDS OF CONDUCT

Employees

3.1 Employees are responsible for ensuring they adhere to the following standards of conduct during the performance of their duties:

i) Employees' actions must be lawful, impartial and in compliance with Service policy.

ii) When dealing with the public, employees' deportment must be professional and they must treat members of the public with courtesy and respect.

iii) Employees must, to the fullest extent possible, be discreet; they must abide by established standards of security during the performance of their duties and functions so that sensitive sources of information, investigations and operational methodologies are not compromised.

iv) Employees must report in a timely, accurate, complete and objective manner all information pertinent to an investigation.

v) Clear distinction must be made between fact, opinion and speculation in reports.

4. SPECIAL INSTRUCTIONS

Section 2(d) Approval

4.1 The Minister will be consulted before undertaking an investigation under subsection 2(d) of the CSIS Act beyond the collection of open information (OPS-100 to OPS-105, "Targeting - Section 12 CSIS Act")

Lawful Advocacy Protest and Dissent

4.2 If, in the course of an investigation of a defined threat to the security of Canada, it becomes necessary to conduct inquiries regarding persons or groups involved in lawful advocacy, protest or dissent, such action will only be undertaken after senior level authorization.

Rule of Law

4.3 When there is uncertainty concerning the lawfulness of an operation or technique, the issue must be referred to the appropriate Regional or Branch Director General for direction.

Unlawful Activity
4.4 When an employee learns of unlawful activity during the performance of his or her duties and functions, they must advise their supervisor.

4.4.1 See also "Authorized Disclosure of Operational Information and Intelligence", (OPS-601 to OPS-603)

5. GUIDELINES FOR OPERATIONAL INTERVIEWS

Identification

5.1 At the outset of an interview, employees must identify themselves as employees of the Canadian Security Intelligence

Informing Interviewee

5.2 Employees must explain the purpose of each interview to the interviewee and provide clarification when asked, as fully as operational and security of information interests allow.

Focus of Interview

5.3 Employees must respect the interviewee's privacy and ensure that the focus of an interview clearly remains on issues relevant to the Service's interests.

Concerns of Immigrants

5.4 Some immigrants to Canada come from countries with a history of human rights violations by police and security officials. When dealing with such persons, employees should be sensitive to the fears or attitudes which often result from prior association with police and security officials.

Threats or Promises

5.5 While conducting interviews employees must not:

i) make threats of any nature for the purpose of intimidating any person into co-operating with the Service;

iii) place the subject of an interview at risk or jeopardize their reputation at their place of work or in their community.

Personal Opinion

5.6 Employees must refrain from offering personal opinions on sensitive issues which could lead to unnecessary confrontation or controversy.

Controversy

5.7 If there is a probability that a complaint may be made or public controversy may ensue as a result of contact with a Service employee, the appropriate Regional or Headquarters DG must be advised immediately.

6. PREPARATION FOR OPERATIONAL INTERVIEWS
6.1 Employees must be adequately prepared before conducting an interview.

6.1.1 Employees should pre-determine their objectives for an interview and identify any assistance they may require from other employees or sections.

6.1.2 When arranging an interview, employees must:

i) consider any social, religious or ethnic issues that may have a bearing on how or where or when the interview may be conducted;

ii) when possible, arrange interviews at the convenience of the interviewee; and,

iii) consider any security problems that may arise and choose a location that affords the appropriate level of privacy or protection.

7. CONDUCTING OPERATIONAL INTERVIEWS

7.1 At the onset of an interview employees should stress the confidential nature of the interview.

Sensitive Issues

7.3 Investigations often require that employees pose very sensitive and personal questions to an interviewee. Employees must be prepared to explain the relevance of questions on sensitive subjects as fully as operational interests allow.

Community Interviews

7.4 When interviews are conducted with leaders of communities and/or interest groups concerning threats to the security of Canada that may affect their community, employees must emphasize that the threat is being investigated and not the community itself.

Identification

7.5 In keeping with the intent of the Community Interview Program, employees involved in community interviews shall identify themselves as employees of the Canadian Security Intelligence Service.

Cooperation is Voluntary

7.6 Employees, when conducting interviews under the auspices of the Community Interview Program, shall at
the outset of the interview explain the purpose of the interview and inform the interviewee that cooperation with
the Service is voluntary.

Presence of Counsel

7.7 Individuals may wish to have legal counsel or other persons (e.g. a family member, friend or adviser) with
them during an interview.

7.7.1 Employees should proceed with the interview unless they believe that it is not in the Service's interests to
do so.

Hostile Interview Subjects

7.8 Investigators may encounter persons who may attempt or are suspected of attempting to deceive,
manipulate, intimidate or otherwise obstruct a lawful investigation by the Service.

7.8.1 When possible, consult your supervisor beforehand and do not conduct these interviews alone.

7.8.2 Investigators concerned with their personal safety may request the presence or assistance of the police of
jurisdiction with the approval of the appropriate DDG, Operations.

7.8.3 Contact with such persons, including full details as to why the individual is considered to be hostile should
be documented on the appropriate file.

8. RECORDING OF OPERATIONAL INTERVIEWS

Electronic Recordings

8.1 If an interviewee wishes to electronically record the interview, the employee should proceed unless there are
compelling reasons not to.

8.1.2 The fact that the interview was recorded by the interviewee should be documented on the appropriate file.

Notes

8.2 Employees should make accurate notes of all interviews.

8.2.1 If note taking during an interview is not possible, do so at the earliest opportunity. See Service policy on
"Operational Notes", OPG-217.

9. COURT SUMMONS / SUBPOENAS
Related to Duties and Functions under the CSIS Act

9.1 Any employee who receives a summons or subpoena related to the performance of duties and functions under the CSIS Act must report it immediately to their respective Director General with a copy to the HQ or Regional Internal Security Representative.

Not Related to Duties and Functions under the CSIS Act

9.2 Any employee who receives a summons or subpoena outside the performance of duties and functions under the CSIS Act are to refer to SEC-202, "Personnel Security: Disclosure of Identity and Use of Identifying Documents" for direction.

2003-08-29
SECRET
OPS-202 CONDUCT OF OPERATIONS - FUNDAMENTAL INSTITUTIONS OF SOCIETY

1. INTRODUCTION

Policy Objective

1.1 The foundation of Canadian democracy consists of fundamental societal institutions which depend on individual rights and freedoms to function properly. Primary among these institutions are those in the academic, political, religious, media and trade union fields.

1.2 In the conduct of operations involving, or associated with, these institutions, sensitivities may surface regarding the propriety of the investigation or the disquieting effect investigations may have on the institution or on the civil liberties of individuals.

1.3 The objective of this policy is to detail the policy and guidelines which govern contact with representatives of these fundamental institutions of society.

Scope

1.4 This policy, in conjunction with OPS-201, "Conduct of Operations - General", provides the principles and standards by which all contact with representatives of fundamental institutions of our society will be governed, with the exception of the level of authority required for enquiries under the Security Screening program (see paragraph 4.1).

Authorities and References

1.5 All authorities and references listed in OPS-201, "Conduct of Operations - General", apply to this policy.

Definitions

1.6 For reference purposes, definitions of fundamental terms have been provided in OPS-201, Appendix 1.

2. PRINCIPLES

2.1 All CSIS operations will be governed by the following principles:

- The rule of law must be observed.
- The investigative means must be proportional to the gravity and imminence of the threat.
- The need to use intrusive investigative techniques must be weighed against possible damage to civil liberties or to fundamental social institutions.
- The more intrusive the investigative technique, the higher the authority required to approve its use.
- The least intrusive investigative methods must be used first, except in emergency situations or where less intrusive investigative techniques would not be proportionate to the gravity and imminence of the threat.

3. MANAGEMENT AND CONTROL OF INVESTIGATIONS
3.1 While guided by the principle that there are no sanctuaries from authorized investigations, special care must be taken in the management and control of investigations which impact on, or appear to impact on, fundamental institutions of our society.

3.1.1 Senior level authorization appropriate to the nature of the investigation and its relationship to the institution involved is required.

4. GENERAL GUIDELINES

Security Screening

4.1 The investigation or interview, under section 12 of the CSIS Act, of representatives of fundamental institutions is potentially more controversial than interviewing such persons as references in security screening investigations. Consequently, the level of authority for security screening enquiries may be at less senior levels.

4.1.1 The Director General of Security Screening must provide guidelines on appropriate authorization levels for contact by security screening investigators with representatives of fundamental institutions.

Controversy

4.2 If any situation involving the Service and a fundamental institution may become controversial, the appropriate Regional and Headquarters DG must be advised.

4.2.1 With the exception of paragraph 4.2.2, the Headquarters DG must advise the Deputy Director Operations via the Assistant Director Operations (ADO) of such controversy and, if directed to do so, prepare a brief for the Director.

4.2.2 Regional DGs must advise the ADO whenever a security screening investigation is to be conducted involving senior public officials or other prominent persons or where there is potential for public controversy.

Human Sources

4.3 For specific direction on the use of human sources under direction in investigations which impact on, or appear to impact on, fundamental institutions, see Human Source policy, "Special Restrictions", OPS-206.

4.4 DGs may delegate any of their authority under the Human Source policy, (OPS-204 to OPS-208) to the DDG, Operations.

5. ACADEMIC INSTITUTIONS

Approvals and Advice

5.1 The Government of Canada and the Service recognize that post secondary institutions are very special places that depend on the free flow of ideas.

5.1.1 It is recognized that, on occasion, the security of Canada requires investigation on campus. Consequently, all operational interviews, queries or surveillance on a campus must have prior approval by the Regional or Headquarters Director General.

Incidental Contact

5.2 If, during the course of physical surveillance, a target travels to a campus, surveillance should not be
terminated if there is reason to believe that valuable intelligence may be lost.

5.2.1 Should surveillance continue, the appropriate Regional DG must be advised immediately.

5.2.2 Follow-up interviews or other enquiries relating to surveillance mentioned in paragraph 5.2 above must be approved by the Regional Director General.

Traversing a Campus

5.3 Surveillance of a target passing through a campus en route to another destination does not require senior level approval.

5.3.1 The occurrence must be noted on file.

Security Screening Investigations

5.4 Ministerial Approval is not required to conduct a security screening investigation at a post-secondary educational institution.

5.4.1 Security screening investigations at post-secondary educational institutions will not be used as a pretext to conduct other Service investigations. See OPS-108, "Government Security Screening", OPS-109, "Immigration Security Screening" and OPS-110, "Citizenship Security Screening".

6. POLITICAL INSTITUTIONS

Levels of Approval

6.1 Operational contact with persons representing political institutions, with the exception of security screening investigations, must receive prior approval as noted below.

6.1.1 Whenever possible interviews should be conducted outside of the precincts of parliament.

Director

6.2 The Director must approve all contact with the Governor General, Prime Minister, Lieutenant Governors, provincial Premiers, federal or provincial cabinet Ministers or Clerk of the Privy Council.

Directors General

6.3 The Headquarters or Regional Director General, as appropriate, must approve any contact with Deputy Ministers, Legislators, Chiefs of Staff or other representatives of political institutions, on a matter under section 12 of the CSIS Act.

6.3.1 The Director must be advised of any anticipated contact with a Federal Deputy Minister.

6.3.2 Contact with persons in executive positions in the offices mentioned, such as Press Secretary, Executive Assistant or such similar positions must be approved by the appropriate Regional or Headquarters DG or their
delegate.

Federal Parliamentary Precincts

6.4 Operations or operational interviews by the Service within parliamentary precincts must be approved by the Solicitor General of Canada and subsequently by the Speaker of the House.

6.4.1 The Deputy Director, Operations (DDO) may authorize an interview within the federal parliamentary precincts provided the subject matter of the interview does not infringe on the privilege of members of parliament.

Provincial Parliamentary Precincts

6.5 Operations and operational interviews within provincial parliamentary precincts must be approved by the Regional DG and subsequently by the Speaker of the House (or equivalent) prior to beginning the operational activity.

Public Meetings

6.6 Employees must not attend public meetings of recognized political parties for the purpose of obtaining information in support of an investigation unless authorized to do so by a DDG Operations or where there is an immediate operational need.

6.6.1 If an employee attends a political meeting due to an immediate operational need, the DG must be advised as soon as possible.

Contact with Elected Municipal Officials

6.7 Employees must obtain the approval of a Regional DG prior to any operational contact with an elected municipal official.

7. MEDIA

Levels of Approval

7.1 Operational contact with members of the media must be approved by the appropriate Regional or Headquarters DG.

7.2 Requests for information or comments from the Service by the media must be referred to the appropriate regional or branch Director General.

8. RELIGIOUS INSTITUTIONS

Level of Approval

8.1 The appropriate Regional or Headquarters DG must be advised of operational contact with members of the clergy or other person officially representing a religious institution when the potential for controversy exists.
9. TRADE UNIONS

Level of Approval

9.1 Operational contact with a person who is acting in an official union capacity must be approved by the appropriate Regional or Headquarters DG.

10. THE JUDICIARY

Level of Approval

10.1 All contact with members of the judiciary (judges at the higher court level) to request operational assistance or to respond to a query must receive prior approval from the Deputy Director, Operations (DDO).

NOTE: Employees should be aware that members of the judiciary may decline involvement in any security intelligence investigation that may call into question their objectivity in the performance of their duties.

2001-10-05
SECRET
OPS-217 OPERATIONAL NOTES

1. INTRODUCTION

Policy Objective

1.1 All operational information gathered by employees pursuant to their duties and functions under the CSIS Act is potentially part of the record of the Service.

1.2 Notes serve as a temporary storage medium for operational information which enables employees to accurately recall an event or the details of information acquired in order that information relevant to the mandated interests of the Service may be accurately reported and analyzed.

1.3 Once the information has been subjected to preliminary analysis and a decision taken that it is to be retained, it falls under the provisions of the Access to Information Act, the Privacy Act and the National Archives Act.

Scope

1.4 This policy provides the principles for the handling and retention of operational notes, hereafter referred to as notes, made during the collection of information related to the Service’s mandate.

1.5 This policy also bridges the requirements of the policies referred to in the "References" section with the aforementioned principles. Emphasis is placed on the security provisions of the CSIS Security Manual (SEC), Part 400, "Security of Information."

Authorities

1.6 CSIS - RCMP Memorandum of Understanding
1.7 Treasury Board: Government Security Policy and Standards (GSP)
1.8 Security of Information Act

References

1.9 CSIS Security Manual (SEC) - "Security of Information"
1.10 CSIS Administration Manual
ADM-403, "Requests: Access To Information and Privacy"
ADM-601, "Information Holdings Policy"
1.11 CSIS Operations Manual (OM)
OPS-601 to OPS-603, "Authorized Disclosure of Operational Information and Intelligence"

OPS-201, "Conduct of Operations - General" and OPS-202, "Conduct of Operations - Fundamental Institutions of Society"

Definitions

1.12 Operational Notes: Any rough note, preliminary draft, drawing, diagram, photograph, calculation, audio or video recording, electronically stored information or other material made by an employee which is to be used in the preparation of a record of the Service.

1.13 Operational Report: A written account or description of investigative activity that contains mandated information and is retained pursuant to the CSIS Act.

2. PRINCIPLES AND RESPONSIBILITIES

Reporting of Information

2.1 Employees are responsible for consolidating, analysing and reporting all information of mandated interest contained in their notes.

Sensitivity of Notes

2.2 Operational notes routinely contain:

-- Security intelligence information which, if compromised, could cause injury to the national interest, jeopardize operations, reveal sources or undermine the effectiveness of the Service;

-- Personal information on individuals which, if compromised, could cause personal harm to that individual.

Security of Notes

2.3 The following principles for the security of notes must be adhered to at all times in accordance with the security standards established in Part 400 of the Security Manual (SEC), "Security of Information":

-- When not in use, classified and designated information including notes, must be stored in security containers approved for the level at which the information is classified or designated.

-- Each employee is responsible for ensuring that all classified and designated information, including notes under his or her control is properly stored, and that classified waste has been shredded at the end of each working day or if the office is left unattended for an extended period of time.

-- Employees must ensure that they safeguard and maintain direct control over classified and designated information that they transport outside the applicable secure zone.

-- Only briefcases approved by Headquarters Internal Security Branch (IS) shall be used for this purpose and they must be locked and tagged with a forwarding return address.

-- Documents may be held overnight in a secure briefcase and the briefcase held under the employee's direct
control; however, every effort shall be made to use Service security containers where available.

Destruction of Notes

2.4 All relevant information from notes must be transcribed to a report at the earliest opportunity.

2.4.1 Notes shall then be destroyed unless it is necessary to retain them for purposes described in paragraph 3.5 of this policy.

Evidentiary Situations

2.5 Although the Service does not normally collect evidence for criminal investigations, employees may, during the course of their duties, acquire information relevant to the investigation of unlawful activity of a serious nature.

2.5.1 In exceptional circumstances an employee's evidence, supported by their notes, may be required by police. See paragraph 3.6 of this policy.

Retention of Information

2.6 Information that is contained in notes shall not be deemed to be a record until it is retained by the Service.

2.6.1 All records are subject to Information Management Branch policy and procedures.

3. GUIDELINES

Note Taking

3.1 Employees may temporarily record information in the form of notes while conducting operational activities such as research, interviews (OPS-201 and OPS-202, "Conduct of Operations"), surveillance or other activities related to, or in support of, an investigation.

Format of Notes

3.2 To afford some protection to sensitive information in the event of the loss or theft of notes, employees should avoid:

PSU Notes

3.3 Notes taken by Physical Surveillance Unit (PSU) personnel must also comply with whatever additional procedures may be established by Operations, Operations Support Branch (OS).
Reporting of Mandated Information

3.4 Notes must be reviewed to ensure information mandated under sections 12, 15, 16 of the *CSIS Act* and subsection 19(2) of the *CSIS Act* is reported.

Destruction of Notes

3.5 Once the relevant information is reported, the notes must be destroyed, except in the following circumstances:

-- When information in notes, such as a sketch or diagram, cannot be transcribed into a report, the relevant portion of the notes may be retained on file;

-- When information contained in the notes may be crucial to the investigation of an unlawful act of a serious nature and employees may require their notes to refresh their memories prior to recounting the facts of an event.

NOTE: "Unlawful activity of a serious nature" is any criminal act that poses a threat to life or property and is an indictable offence or is one on which the crown may elect to proceed by indictment. (i.e. Activities relating to murder, bombing or hijacking)

3.6 Employees must advise their supervisor if they believe they have acquired information of possible evidentiary value and indicate if this information is supported by their notes.

3.6.1 The decision to bring this information to the attention of the police and the subsequent retention of the notes shall be made by the Regional Director General.

3.6.2 All such action must be in compliance with Service policy on "Authorized Disclosure of Operational Information and Intelligence", OPS-601 to OPS-603.

Use of Notes in Exceptional Circumstances

3.7 In exceptional circumstances, where the police of jurisdiction are unable to obtain their own independent evidence, the evidence of an employee, supported by the employee's notes, may be crucial to the successful prosecution of a serious criminal case.

3.7.1 Such circumstances are subject to:

-- service policy on the "Authorized Disclosure of Operational Information and Intelligence" (OPS-601 to OPS-603); and,

-- the CSIS/RCMP Memorandum of Understanding (MOU) if the investigation is within the mandate of the RCMP.

Retention of Notes

3.8 Notes that have been determined to be of evidentiary value must be placed in a sealed envelope and retained on the related operational file.

3.8.1 When notes are retained and used to support an employee's evidence, consideration shall be given to the protection of non-related information that may be contained in the same notebook or other notes.

3.8.2 If the employee is required to produce these notes in court the protection of such information shall be the
subject of agreement between the Service and the police or Crown Prosecutor.

3.8.3 Final disposition of notes shall be the subject of agreement between the Service and the police or Crown Prosecutor.

2002-03-14

SECRET
Custodial interviews of Omar Ahmed KHADR

1) This report summarizes interviews of US Department of Defense detainee, Omar Ahmed KHADR (DOB: 1986 09 19, Scarborough, Canada), by [blurred] investigators. The interviews were conducted on 2003 09 22 (Monday) 1430 hrs and 2003 09 25 (Thursday) 1100 hrs at United States Naval Base, Guantanamo Bay (GITMO), Cuba. Omar KHADR is to be considered a source of unknown reliability.

2) Throughout both interviews, Omar KHADR (OK) attempted to convince the investigators that his previous statements outlining his and his family's involvement with Al Qaida were false. OK maintained that his statements were the result of his torture by American interrogators following his capture in Afghanistan. The investigators asked OK to describe the type of torture he endured, he replied 'listening to other people scream.' We then challenged that his current denials contradict irrefutable evidence, such as the video made by Abu LAITH showing OK assembling improvised explosive devices (IED). OK claimed that such information was fabricated by the Americans to implicate him in the killing of an American soldier. OK stated that because he was the sole survivor of the assault, the Americans are using him as a scapegoat.

3) OK stated that he was last in Canada between 2001 02 14 - 2001 05. At the time, he was 15 years old. He claims to have travelled with his mother, Maha ELSAMNAH, his brothers Abdul Rahman KHADR (ARK), and Abdulkareem KHADR, his sisters Maryam KHADR and Zeinab KHADR, and Zeinab's daughter, Safia.
During this visit, the family stayed at the home of OK’s grandparents, Mohamed and Fatima ELSAMNAH. OK was asked what the purpose of this trip to Canada? Hereplied for Safia to undergo surgery. OK was asked whether an alternate reason was to fundraise for his father’s organization, HEALTH AND EDUCATION PROJECT INTERNATIONAL (HEPI)? He replied it was possible, however, he claimed not to remember. He stated that all of HEPI raised all its money in Canada and Bahrain.

OK was asked to explain the fundraising support base in Bahrain? He claimed not to know, simply stating that his family had several close associates in this country. While in Canada, OK recalled frequenting the SALAHeddin ISLAMIC CENTRE, as well as Mosques in Mississauga and Waterloo with his mother. OK claimed to have never visited Hamilton or St Catharines. OK was asked whom he associated with during this visit? He indicated that he spent most of his time with his cousin, Bilal, whom he considers his closest friend in Canada. He further stated that ARK hung around with numerous friends during this visit.

However, because of the age difference between him and his brother (who was 19 at the time), Omar KHADR was discouraged from hanging out with ARK and his friends. OK stated that his other brother, Abdullah KHADR, has not been back to Canada since 1990.

When asked about the nature of travel to the region, OK claimed it was simply to spend time with ARK, but refused to elaborate on specifics. OK furthered that because he was only 13 years old at the time, his older brother did not want him hanging around with him and . Furthermore, he stated that ARK and were often away from the family home (NFI). We informed OK that the Service was aware that had spent time at a training camp during this visit. OK claimed to have no such knowledge of such camps. When challenged on this point, OK instructed the investigators to speak with ARK. OK stated that he was aware ARK was also detained at GITMO.
6) The investigators queried OK about other Canadians who had visited the KHADR family in Pakistan or Afghanistan. OK recalled Hilmy EL-SHERIF and Abdullah ALMALKI, merely stating that they had worked with his father. OK further recognized a photograph of Mahmoud JABALLAH, claiming he was a friend of his father. OK would not elaborate on the nature of any of these relationships.

9) OK stated that he has received separate letters from Maha ELSAMNAH and Zeinab KHADR within the past month. According to OK, both letters claim that the remaining members of the
family, including ASK and Abdullah KHADR, are safe and living together on a farm in rural Pakistan. OK claimed that the location of this farm, or the closest urban centre, was not divulged in the letter. In her letter to OK, Zeinab mentioned that she had recently separated from Yacoub AL - Bahr. However, ASK had arranged for Zeinab to remarry an unidentified person. OK stated that he was saddened by this news, as he felt that every person whom his father set Zeinab up with ended up mistreating her.

Omar KHADR (DPOB: 1986 09 19, Scarborough, Canada)
Detainee
United States Naval Base
Guantanamo Bay (GITMO), Cuba

OK consistently denied any knowledge of anything related to Islamic extremism and AL QAIDA. Despite being repeatedly challenged on these denials, he maintained that any names, events, or locations he had previously divulged in interviews were put in his mind by the Americans and were the product of torture. In reference to his previous custodial interview with CSIS, conducted by [REDACTED] on 2003 02 13 - 2003 02 16, OK repeatedly claimed that he believed [REDACTED] was an American interrogator posing as a Canadian. OK claims he initially told [REDACTED] the same story he told previous interrogators to stay consistent, again contending it was forced out of him under duress.