Air India Flight 182

A Canadian Tragedy

VOLUME ONE

The Overview

Cat. No: CP32-89/2-2010E
ISBN: 978-0-660-19926-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
K1A 0S5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
Publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

Commission of Inquiry
into the Investigation of
the Bombing of Air India
Flight 182

Commission d'enquête relative
aux mesures d'investigation prises
à la suite de l'attentat à la bombe
commis contre le vol 182 d'Air India

June 2010

To Her Excellency
The Governor General in Council

May it please your Excellency:

As Commissioner appointed by Order in Council P.C. 2006-293 issued on May 1, 2006 pursuant to Part 1 of the *Inquiries Act,* and in accordance with the Terms of Reference assigned therein, I respectfully submit this final report entitled "Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182". The report comprises: Volume I, an Overview and guide to the reader; and Volumes II to V covering the Commission's findings relating to all seven specific questions in the Terms of Reference. Associated with the report are four volumes of academic studies addressing various aspects of the Commission's work.

John C. Major, C.C., Q.C.
Commissioner

P.O. Box 1298, Station "B", Ottawa, Ontario / C.P. 1298, succursale "B" Ottawa (Ontario)
K1P 5R3
Tel. / Tél. : 613 992-1834 Fax / Télécopieur : 613 995-3506

Canada

TERMS OF REFERENCE

Her Excellency the Governor General in Council, on the recommendation of the Prime Minister, hereby directs that a Commission do issue under Part I of the *Inquiries Act* and under the Great Seal of Canada appointing the Honourable John C. Major, Q.C., as Commissioner to conduct an inquiry into the investigation of the bombing of Air India Flight 182 (the "Inquiry"), which Commission shall direct

a. the Commissioner to conduct the Inquiry as he considers appropriate with respect to accepting as conclusive or giving weight to the findings of other examinations of the circumstances surrounding the bombing of Air India Flight 182, including

   i. the report of the Honourable Bob Rae entitled *Lessons to Be Learned* of November 23, 2005,

   ii. proceedings before the superior courts of British Columbia,

   iii. the 1991-1992 Security Intelligence Review Committee review of Canadian Security Intelligence Service activities in regard to the destruction of Air India Flight 182,

   iv. the report of the Honourable Mr. Justice B.N. Kirpal of the High Court of Delhi of February 26, 1986,

   v. the Aviation Occurrence Report of the Canadian Aviation Safety Board into the crash involving Air India Flight 182 of January 22, 1986,

   vi. the 1985 report of Blair Seaborn entitled *Security Arrangements Affecting Airports and Airlines in Canada*, and

   vii. the reports prepared by the Independent Advisory Panel assigned by the Minister of Transport to review the provisions of the *Canadian Air Transport Security Authority Act*, the operations of the Canadian Air Transport Security Authority and other matters relating to aviation security;

b. the Commissioner to conduct the Inquiry specifically for the purpose of making findings and recommendations with respect to the following, namely,

i. if there were deficiencies in the assessment by Canadian government officials of the potential threat posed by Sikh terrorism before or after 1985, or in their response to that threat, whether any changes in practice or legislation are required to prevent the recurrence of similar deficiencies in the assessment of terrorist threats in the future,

ii. if there were problems in the effective cooperation between government departments and agencies, including the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, in the investigation of the bombing of Air India Flight 182, either before or after June 23, 1985, whether any changes In practice or legislation are required to prevent the recurrence of similar problems of cooperation in the investigation of terrorism offences in the future,

iii. the manner in which the Canadian government should address the challenge, as revealed by the investigation and prosecutions in the Air India matter, of establishing a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial,

iv. whether Canada's existing legal framework provides adequate constraints on terrorist financing in, from or through Canada, including constraints on the use or misuse of funds from charitable organizations,

v. whether existing practices or legislation provide adequate protection for witnesses against intimidation in the course of the investigation or prosecution of terrorism cases,

vi. whether the unique challenges presented by the prosecution of terrorism cases, as revealed by the prosecutions in the Air India matter, are adequately addressed by existing practices or legislation and, if not, the changes in practice or legislation that are required to address these challenges, including whether there is merit in having terrorism cases heard by a panel of three judges, and

vii. whether further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, particularly those relating to the screening of passengers and their baggage;

c. the Commissioner to conduct the Inquiry under the name of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182;

d. that the Commissioner be authorized to adopt any procedures and methods that he may consider expedient for the proper conduct of the Inquiry, and to sit at any times and in any places in or outside Canada that he may decide;

e. that the Commissioner be authorized to conduct consultations in relation to the Inquiry as he sees fit;

f. that the Commissioner be authorized to grant to the families of the victims of the Air India Flight 182 bombing an opportunity for appropriate participation in the Inquiry;

g. that the Commissioner be authorized to recommend to the Clerk of the Privy Council that funding be provided, in accordance with approved guidelines respecting rates of remuneration and reimbursement and the assessment of accounts, to ensure the appropriate participation of the families of the victims of the Air India Flight 182 bombing;

h. that the Commissioner be authorized to grant to any other person who satisfies him that he or she has a substantial and direct interest in the subject-matter of the Inquiry an opportunity for appropriate participation in the Inquiry;

i. that the Commissioner be authorized to recommend to the Clerk of the Privy Council that funding be provided, in accordance with approved guidelines respecting rates of remuneration and reimbursement and the assessment of accounts, to ensure the appropriate participation of any party granted standing under paragraph (h), to the extent of the party's interest, where in the Commissioner's view the party would not otherwise be able to participate in the Inquiry;

j. that the Commissioner be authorized to rent any space and facilities that may be required for the purposes of the Inquiry, in accordance with Treasury Board policies;

k. the Commissioner to use the automated litigation support program specified by the Attorney General of Canada and to rely, to the greatest extent possible, on documents that have been previously identified for use in Canadian criminal proceedings arising from the bombing of Air India Flight 182, and to consult with records management officials within the Privy Council Office on the use of standards and systems that are specifically designed for the purpose of managing records;

l. that the Commissioner be authorized to engage the services of any experts and other persons referred to in section 11 of the *Inquiries Act*, at rates of remuneration and reimbursement approved by the Treasury Board;

m. the Commissioner, in conducting the Inquiry, to take all steps necessary to prevent disclosure of information which, if it were disclosed, could, in the opinion of the Commissioner, be injurious to international relations, national defence or national security and to conduct the proceedings in accordance with the following procedures, namely,

    i. on the request of the Attorney General of Canada, the Commissioner shall receive information *in camera* and in the absence of any party and their counsel if, in the opinion of the Commissioner, the disclosure of that information could be injurious to international relations, national defence or national security,

    ii. the Commissioner may release a part or a summary of the information received *in camera*, if, in the opinion of the Commissioner, its disclosure would not be injurious to international relations, national defence or national security, and shall provide the Attorney General of Canada with an opportunity to make submissions regarding international relations, national defence or national security prior to any release of a part or a summary of information received *in camera*,

    iii. if the Commissioner concludes that, contrary to the submissions of the Attorney General of Canada referred to in subparagraph (ii), disclosure of a part or a summary of information received *in camera* would not be injurious to international relations, national defence or national

security, he shall so notify the Attorney General of Canada, which notice shall constitute notice under section 38.0 of the *Canada Evidence Act*,

iv. the Commissioner shall provide the Attorney General of Canada with an opportunity to make submissions regarding international relations, national defence or national security with respect to any reports that are intended for release to the public prior to submitting such reports to the Governor in Council, and

v. if the Commissioner concludes that, contrary to the submissions of the Attorney General of Canada referred to in subparagraph (iv), disclosureof information contained in reports intended for release to the public would not be injurious to international relations, national defence or national security, he shall so notify the Attorney General of Canada, which notice shall constitute notice under section 38.01 of the *Canada Evidence Act*;

n. that nothing in that Commission shall be construed as limiting the application of the provisions of the *Canada Evidence Act*;

o. the Commissioner to follow established security procedures, including the requirements of the *Government Security Policy*, with respect to persons engaged pursuant to section 11 of the *Inquiries Act* and the handling of information at all stages of the Inquiry;

p. the Commissioner to perform his duties without expressing any conclusion or recommendation regarding the civil or criminal liability of any person or organization;

q. the Commissioner to perform his duties in such a way as to ensure that the conduct of the Inquiry does not jeopardize any ongoing criminal investigation or criminal proceeding;

r. the Commissioner to file the papers and records of the Inquiry with the Clerk of the Privy Council as soon as reasonably possible after the conclusion of the Inquiry;

s. the Commissioner to submit a report or reports, simultaneously in both official languages, to the Governor in Council; and

t. the Commissioner to ensure that members of the public can, simultaneously in both official languages, communicate with, and obtain services from it, including transcripts of proceedings if made available to the public.

AIR INDIA FLIGHT 182: A CANADIAN TRAGEDY

REPORT TABLE OF CONTENTS

VOLUME THREE
The Relationship between Intelligence and Evidence and the Challenges of Terrorism Prosecutions

VOLUME FOUR
Aviation Security

VOLUME FIVE
Terrorist Financing

READER'S GUIDE
Acronyms and Key Names

VOLUME ONE
THE OVERVIEW

TABLE OF CONTENTS

VOLUME ONE
THE OVERVIEW

CHAPTER I: INTRODUCTION

On June 23, 1985, a bomb explosion killed the 329 passengers and crew of Air India Flight 182 in mid-flight. Fifty-nine minutes earlier, at Tokyo's Narita Airport, two baggage handlers were killed by an explosion from a bomb while offloading luggage from a Canadian Pacific Airlines flight. The luggage had been destined for an Air India flight. Both bombs were planted in suitcases by the same group of Sikh terrorists. Three hundred and thirty-one people were killed.*

There have been two criminal trials. At each, Inderjit Singh Reyat was convicted for manslaughter for his involvement in the explosions, which were found to be part of a criminal conspiracy. In 2005, two accused were acquitted of the crimes. No other persons have been charged.

This remains the largest mass murder in Canadian history, and was the result of a cascading series of errors.

***

This is a large report, covering seven substantive Terms of Reference, and events commencing over twenty years ago.

Its size reflects the ambitious mandate that has been assigned to this Commission, encompassing a review and evaluation of the performance and interactions of government agencies before and after the bombing, along with a request for recommendations in some of the most difficult and complex areas in relation to this country's response to the murderous phenomenon of terrorism.

The size of the report also reflects the Commission's view of its obligation to lay out in comprehensive detail the facts about the Government's preparedness for the possibility of the bombing and for the subsequent post-bombing investigation. At a minimum, this much is owed to the families of the victims and to the Canadian public at large.

Important new facts came to light during the hearings and the documentary review conducted by the Commission. The Commission viewed it as an important part of its mandate to establish the official public record of this event and the Report attempts to do so in a comprehensive fashion.

* The Boeing 747 "Kaniskha" flew into Montreal as Air India Flight 181 and departed as Air India Flight 182.

The Commission's mandate to provide realistic and pragmatic recommendations for complex policy issues means that the portions of the Report devoted to that endeavour must also be detailed, comprehensive and fully informed by the current state of expert understanding in these areas.

This volume is provided for those who want a quick and convenient 'bottom line' discussion of the issues. The Overview is not a substitute for the Report nor is it, strictly speaking, an Executive Summary. It is designed to function as a type of reader's guide to the Report, presenting, in an accessible form, highlights of the major observations and findings in the Report. It does not attempt to condense the Report, but rather to reflect on it, bringing together themes and conclusions based on the larger Report.

This first chapter of this volume is an introduction, to orient the reader to the discussion that follows. It is a high-level capsule summary of some of the findings and conclusions reached by the Commission. Most, but not all, of these conclusions are also discussed in the volume itself and detailed in the body of the Report.

The Past

1.0 Pre-Bombing: Assessment of and Response to the Threat

1.1 Agencies' Preparedness for the Threat of Terrorism

The Government of Canada and its agencies were not prepared for a terrorist act like the bombing of Flight 182.

1.1.1 CSIS

CSIS had been created less than a year before the terrorist attack. At the time, it was still primarily focused on Cold War priorities like counter-espionage. CSIS was poorly trained and under-resourced for counter-terrorism, and what resources existed were focused primarily on threats other than those emanating from Sikh extremism.

Although human sources are the lifeblood of intelligence, CSIS had few, if any, sources in the Sikh community in the pre-bombing period. Its ability to respond to Sikh terrorism was further impaired by unwieldy policies and procedures for wiretaps.

There seemed little sense of purpose to CSIS intelligence gathering in this area. The information gathered from the wiretap on Talwinder Singh Parmar,[1] obtained after months of delay, was not processed effectively or in a timely manner; it was ignored by CSIS investigators and, to compound the problem,

---

1 The person who, at the time, was thought to be the leader of a terrorist group.

the tapes of the wiretap were prematurely and unthinkingly erased, even after the bombing. Surveillance on Parmar was intermittent and ineffective. Even though a surveillance team was present when Parmar and his associates detonated a device in the woods near Duncan, causing a loud explosive sound, the sound was misinterpreted and the surveillance report was ignored. Despite the remarkable and unambiguously alarming behaviour witnessed by the surveillance team, further surveillance was called off on the very day of the bombing in order to follow a Cold War target.

Most importantly, however, the CSIS analysis of the threat posed by Sikh extremism was handicapped because it was not provided with key intelligence information in the possession of the RCMP and the Communications Security Establishment (CSE).

1.1.2 RCMP

In the wake of the creation of CSIS, the RCMP attempted to reconstitute its intelligence capacity on the basis of a misguided emphasis on its mandate to investigate "security offences" for criminal purposes. The decentralized RCMP structure was not easily adaptable to the needs of intelligence gathering and analysis. Little thought was put into the reporting relationships and requirements that would allow for effective collection and analysis of intelligence information. The result was that, at best, the RCMP duplicated CSIS intelligence gathering and, at worst, it failed to report important information that CSIS might have been able to use in its intelligence analysis.

Despite its aspirations to be an intelligence-gathering agency, the RCMP showed a surprising lack of understanding of the nature or purpose of intelligence gathering. The RCMP neglected to consider, let alone report or pass on to CSIS, important information to which it had access from local forces, such as the Khurana information about a comment by a Sikh extremist leader in mid-June 1985, that something would be done in two weeks to address the absence of attacks on Indian interests. The RCMP focused to such an extent on gathering information of evidentiary value or admissibility that it prematurely dismissed information that was useful intelligence. Often, the Force's subjective judgement of credibility for evidentiary use was inadequate even for criminal law purposes, let alone as a justification for failing to report threat information to other agencies.

The failure to understand the value of intelligence and the importance of reporting meant that, when information was received by the RCMP, CSIS was often not given a proper report. This is what happened with the November Plot information about Sikh extremists who were planning to bomb one, and possibly two, Air India planes in November 1984. This is also what happened when, unforgivably, the RCMP did not forward to CSIS the June 1st Telex that set out Air India's own intelligence, forecasting a June terrorist attempt to bomb an Air India flight by means of explosives hidden in checked baggage. This fact, which the RCMP did not reveal to the Honorable Bob Rae in 2005, was uncovered by the Commission.

1.1.3 Transport Canada

As of the late 1970s, Transport Canada was aware of a major gap in this country's civil aviation security regime.

It was aware that the security plans in place focused on hijacking, even though sabotage by means of concealed explosives was the greater and more urgent risk. It was aware that Air India's security plan was inadequate to deal with the risk of sabotage by means of explosives and had even prepared a series of draft regulations capable of responding to some of these problems, but did not push for regulatory change until after the bombing.

Under the regulatory scheme in place, the airlines had responsibility for implementing many of the key security measures. However, Transport Canada had few, if any, mechanisms by which to ensure that the airlines actually performed their functions effectively. It stood by, as a lax and ineffective security culture permeated both private security and RCMP protective policing security arrangements at airports.

On the day of the bombing, an unauthorized summer employee was able to get on board the ill-fated Air India plane and circulate throughout the aircraft unchallenged. Throughout the pre-bombing period, and even thereafter, security checks were so lax that persons with known associations to Sikh extremist groups had access to numerous highly sensitive areas at Vancouver International Airport.

1.1.4 RCMP Protective Policing

RCMP Protective Policing played an important role in maintaining the security of Canadian airports, but it was afflicted with poor morale and poor policies.

Protective policing was not valued within the structure of the RCMP, and was often left out of the loop in terms of threat information because of the RCMP's failures in gathering and reporting that information. Protective Policing had no analytical capability of its own to assess what information it did receive from the airlines and External Affairs. It was entirely dependent on CSIS and on the RCMP threat assessment processes, both of which regularly conducted their analyses on the basis of incomplete information. Security measures in response to possible threats to aviation were poorly thought-out and not tailored to meet the particular nature of the actual threat. An undue and unreflective reliance on the concept of "specific threat" meant that, in the absence of a same-day phone-in bomb threat, certain types of security responses, including those capable of detecting explosives in registered luggage, were not available. In other circumstances, security measures were mechanically applied to a notional "threat level" rather than being based on an analysis of the actual threat.

On the day of the bombing, despite the heightened threat environment, the RCMP canine bomb sniffing unit, the single most effective means to detect

explosives, was entirely unavailable at Canadian airports because all the police dogs and their handlers were at a training session in Vancouver. This occurred, despite the fact that the RCMP knew of the increased threat to Air India. Included in the intelligence at its command, was the June 1st Telex, which foretold a June attack against an Air India flight. Yet the RCMP permitted its entire canine unit to engage in a training session at the point when the threat was at its highest. The RCMP and Transport Canada concealed and misrepresented this fact, up to and including their submissions to the Honourable Bob Rae in 2005. In Montreal, where a back-up dog was available, it was not even called into the airport until after the plane had departed.

1.1.5 Air India

With the partial privatization of aviation security responsibilities at Canadian airports, Air India was left to devise its own security program. Customer service concerns often trumped security concerns, as Air India's security operations were heavily influenced by the need to speed up screening and to meet strict timelines imposed by management.

Air India subcontracted security duties to private security firms whose employees were poorly trained and poorly compensated. It placed its confidence in technology that was known to be unreliable. Its equipment was not well maintained and was poorly calibrated, with the result that its X-ray screening equipment at Pearson broke down on the day of the bombing after screening only a portion of the checked baggage.

The rest of the baggage was screened by use of a "PD4 sniffer" device. The PD4 sniffer equipment had been demonstrated in tests at Pearson airport to be ineffective in detecting explosives. On the day of the bombing the device was being operated by security staff unfamiliar with it and untrained in its operation.

Despite the detailed advice set out by the Air India intelligence bureau in the June 1st Telex as to the security measures necessary to meet the risk of a terrorist bombing, Air India did not deviate from its existing security plan. Specifically, it did not implement measures suggested in the Telex, such as random physical checks of registered luggage, that were designed to guard against the sort of terrorist plan that caused the bombing of Flight 182.

Neither Transport Canada nor Air India were prepared for the possibility of an unaccompanied interlined bag containing a bomb that could be placed on an Air India flight. On June 22, 1985, those who plotted the Air India bombing successfully used this means of placing the "unaccompanied, infiltrated" bag on Air India Flight 182. Passenger-baggage reconciliation – something that had been successfully implemented in Canada on an *ad hoc* basis prior to the bombing – would have prevented the bomb from being placed on the flight.

Despite the identification of several suspicious bags at Mirabel airport (the first stop after take off from Pearson), cost considerations motivated the decision to allow Flight 182 to depart. The plane was already late, and further delay would have added a cost to Air India in the form of additional airport fees.

1.2 The "Mosaic Effect[2]": Did the Government Have Advance Warning of a Possible Bomb Attack on Flight 182

At the hearings, the Government tried to frame this question in terms of whether government agencies had information about a "specific threat." A great deal of effort was expended in trying to demonstrate that pre-bombing threat information lacked particularity and specificity, as an attempt to provide justification for not employing measures tailored to meet the threat.

Nowhere did this strategy see greater expression and focus than in the Government's efforts to attack the credibility of James Bartleman, who, at the time of the bombing, was Head of the Intelligence Bureau at External Affairs, and subsequently became Lieutenant Governor of Ontario. Bartleman testified that, shortly before the bombing, he saw a highly classified CSE document that indicated that Flight 182 would be targeted by Sikh extremists.

Despite the vigour of the cross examination, Bartleman's testimony, namely that a document he saw led to the conclusion that the weekly Toronto to New Delhi Air India flight was a likely terrorist target remains, in its essence, credible. However, despite the Government's strenuous efforts to make the case, it is simply not accurate that other than Bartleman's testimony, there was nothing to suggest the existence of documents that should have led the Government to have anticipated the bombing of Flight 182 and to have acted to put in place security precautions to minimize the risk. To the contrary, Bartleman's testimony, was neither the only, nor even the most important evidence pointing to precisely that conclusion. The Government strategy and its attack on Bartleman were both misconceived.

The June 1st Telex was detailed and specific: as to the nature of the threat, as to the means likely to be used, and as to the time frame of the danger. It even provided a checklist of potential security measures capable of responding to the threat. The RCMP did not pass the June 1st Telex on to anyone and never did anything about it.

Given what else was known about Sikh extremism in Canada, the contents of the June 1st Telex would, on their own, be enough to justify the Commission's conclusion that the Government was in possession of enough information to

---

2 The "mosaic effect" is the term used by intelligence agencies, often as an argument against the release of information to the public. It suggests that an individual piece of information, though seemingly insignificant on its own, may serve as the missing piece to a puzzle that allows a hostile group see a pattern or draw conclusions about sensitive government secrets. This same process of gathering and piecing together even seemingly insignificant information can equally be exploited to further an agency's own intelligence effort.

understand that there was a high risk of Sikh extremists trying to blow up an Air India plane by means of explosives concealed in checked baggage. Those contents would also, on their own, validate the further conclusion that it is impossible to justify the state of security at that time at Pearson and Mirabel airports, which was totally inadequate to deal with this threat.

But the June 1st Telex was not the only item of new intelligence to come to light in June 1985. After the close of the hearings, the Commission's review of CSE material revealed that CSE was in possession of additional information about threats indicating that during essentially the same time period, security measures substantially similar to those listed in the June 1st Telex were being mandated for Air India operations, inside and outside of India, in light of threats of hijackings and bombings by Sikh extremists. As well, there was information that Indian airports were undertaking security audits in response to these instructions and that the Government of India had recently shown an increased interest in the security of airports against the Sikh terrorist threat in June 1985. Knowledge of the CSE information could have helped dispel the perception of RCMP and Transport Canada officials that threats to Air India, such as the June 1st Telex, were provided to the Canadian Government as a means of obtaining additional security for free. The fact that the Government of India was pursuing anti-sabotage measures similar to those outlined in the June 1st Telex in June 1985 would seem to support the credibility of this threat. There is no record of this information being circulated anywhere within the Canadian Government.

The Commission concludes that, in the hands of a skilled intelligence analyst, the CSE information would, on its own, more than justify a review of the security measures in place at Pearson and Mirabel to determine whether they were adequate to deal with the risk identified in the information.

That, of course is exactly what Bartleman did as a result of the document he testified to having seen. The document he described had more detail, in some respects, than the June 1st Telex or the CSE information. But, even if it were no more detailed than either of those pieces of information, it would have justified Bartleman's reaction of turning to the protective authorities in order to make sure that they were aware of the threat information and had the response in hand.

However, even without Bartleman's document, there was enough information in the hands of various Canadian authorities to make it inexcusable that the system was unable to process that information correctly and ensure that there were adequate security measures in place to deal with the threat. The June 1st Telex, the November Plot information, the CSE information, the fact that the Sikh extremist community in Canada had issued threats against Indian interests and had engaged in violence, and the fact that CSIS suspected that Parmar would engage in terrorist activities, all combine to create a mosaic of information which clearly identified a particularised threat to Air India for the month of June 1985. This constellation of factors should have compelled the Government to tailor and implement security measures to meet this identified threat.

1.3 Conclusion: Pre-Bombing

The arrangements in place at the relevant government agencies in June 1985 were entirely inadequate to deal with the threat of Sikh extremism in general or to anticipate and prevent the bombing of Flight 182.

1.4 Post-Bombing: CSIS/RCMP Cooperation

In the post-bombing period CSIS and RCMP cooperation was poor. Each agency became unduly focused on its own mandate, and this prevented the development of a cooperative and pragmatic approach to the investigation of the bombing. Each agency relied on its inward-looking, silo-oriented understanding of its own mandate to justify its failure to cooperate with the other, and the "big picture" was lost.

1.4.1 CSIS Does Not Collect Evidence

In the aftermath of the bombing, it was CSIS that had the lion's share of information that might be relevant to the investigation of the bombing. Its approach ranged from sporadic attempts at cooperation to frequent retreats into its own independent mandate as a justification for non-involvement. There was a degree of defensiveness and self-justification and even an apparent attempt by CSIS to "solve" the bombing on its own.

Sharing by CSIS was never complete, and much of its reticence was expressed in its mantra: "CSIS does not collect evidence." This accurate statement of fact - that CSIS was not a law enforcement agency and that its mandate was to collect intelligence rather than to support prosecutions - soon lost its original meaning and became a justification for CSIS to withhold information and ignore its potential role as an aid to law enforcement. A variant of this formulation was used to justify CSIS's destruction of the Parmar tapes, though the evidence suggests that the destruction was a result of CSIS's automatic and unthinking application of its erasure procedure, rather than having been done for any ulterior motive. The same justification was invoked to explain the destruction of original notes and tape recordings by CSIS of interviews with "Ms. E", which was one of many failures that served to impair the usefulness of her statements as evidence at the Air India Trial.

On the other hand, CSIS did have some cause to be sceptical of the RCMP's ability to handle sensitive intelligence information. On one occasion, the RCMP included sensitive CSIS information in court documents without CSIS's permission, and thereby endangered CSIS's ongoing operations.

Ultimately, CSIS information was necessary to the prosecution in both the Narita and the Air India trials, for use as evidence and for purposes of disclosure to the defence. This led to ongoing disputes about the use of CSIS information, disputes in which CSIS interests in maintaining the confidentiality of its

intelligence constantly clashed with the needs of the criminal justice system for full disclosure. Each side had difficulty understanding the perspective of the other, and each agency frequently attributed bad faith to the other agency's position.

There is no evidence that CSIS ultimately withheld any relevant information from the RCMP. However, as outlined in the testimony of Crown Prosecutor James Jardine, who is now a provincial Court judge in British Columbia, the process of disclosure was slow, intermittent and acrimonious. CSIS waited until it had absolutely no other choice but to disclose, and the RCMP continued to harbour suspicions that CSIS had information that it had not disclosed.

1.4.2 The Battle over Sources

The most acrimonious disputes between the two agencies occurred in connection with questions of access to sources and the use of their information. CSIS considers human sources to be its most valued assets. The RCMP considers human sources as witnesses as well as informants, and evaluates their information in terms of its evidentiary value at a potential trial.

Despite having few human sources at the outset of the investigation, CSIS did eventually succeed in cultivating a number of sources in the Sikh community. "Mr. A", "Mr. Z", "Ms. D" and "Ms. E" were all sources from the Sikh community, who first spoke with CSIS and were willing to share information with the authorities but only on condition, at least initially, that they not be required to testify.

The RCMP took the position that the criminal investigation took priority, and wanted access to the sources. The RCMP used approaches more suitable to dealing with police informants with a criminal background than to speaking with frightened members of a close-knit ethnic community. Although RCMP investigators tended to discount the credibility of the sources, they nevertheless insisted on exclusive access so as to prevent "contamination" of the witnesses' potential evidence by CSIS. This fear was borne-out in the case of Ms. E, whose hearsay statements were found unreliable at the Air India trial, in part on this basis. As was the case with Mr. A, an equally frequent result was that both agencies lost out when CSIS's access to the source was cut off, but the source refused to cooperate with the RCMP.

Each of "Mr. A", "Mr. Z", "Ms. D" and "Ms. E", along with the publisher Tara Singh Hayer, who was a community contact for CSIS, was treated insensitively by the RCMP. This was especially true in the case of Ms. E, whose life was permanently altered for the worse by her contact with the RCMP – to the point where she refused further contact with the RCMP and feigned memory loss when forced to testify. In the case of "Ms. D" and Tara Singh Hayer, RCMP sloppiness led to disastrous results. For Ms. D, it meant premature entry into a witness protection program that cut her off from her family and that, from her perspective, ruined her life. For Hayer, the result was a failure on the part of the RCMP to provide adequate or effective protection. In 1998, he was murdered in his own garage.

CSIS reacted to the RCMP's mistreatment of CSIS sources with considerable bitterness and dismay. It became an additional reason cited for CSIS's wariness in sharing information with the RCMP. Several skilled CSIS source handlers left the Service in the wake of these episodes.

1.4.3 The RCMP Investigation

The RCMP post-bombing investigation was marred by a number of factors. The investigation was conducted by a task force made up of members seconded from federal units of the RCMP and was short on practical experience investigating serious crimes. The approach taken was a generally unimaginative one, more suitable to the investigation of an ordinary crime than of a terrorist conspiracy, with an overly narrow and premature focus on evidentiary issues.

The task force seemed stymied by the lack of a crime scene and the absence of other usual features of a criminal offence. The Narita bombing, which did have a crime scene and, through the excellent work of the Japanese police, had evidence to link the crime to a specific individual, soon became the focus.

In the late 1980's and early 1990's, RCMP management showed little interest in treating the investigation of the Air India bombing as a conspiracy. Little progress was made using conventional investigative approaches, and the efforts to turn CSIS sources into witnesses or to recruit RCMP sources came up empty. Morale was low and personnel changes were frequent, allowing for little continuity. At one point, the Air India investigation was assigned to a single RCMP investigator, whose focus was on the coordination of attempts to raise the wreckage of the plane from the ocean bottom and on file administration. In this time frame, an attempt was made at E Division to formally shut down the investigation.

Coordination between the investigators and Headquarters was poor and further hampered by dysfunctional lines of reporting. The B.C. investigators became defensive and spent much of their investigative effort attempting to justify their early dismissal of the relevance of episodes like the Khurana Tapes and the November Plot or their denial of the usefulness of potential sources of information like Mr. A, or Pushpinder Singh.

By the mid-1990's, the police investigation was at an impasse and serious consideration was again given to winding it up. Rather than admitting defeat, the RCMP decided in 1995 to review and reinvigorate the investigation, and charges were eventually laid. The investigation then proceeded largely, and at times exclusively, on the basis of information generated by CSIS in the pre-bombing and immediate post-bombing periods. Many of the most important witnesses at trial were CSIS sources who had been taken over by the RCMP. The prosecution failed because of credibility and evidentiary problems arising from the testimony of these witnesses.

1.5 Conclusion: Post-Bombing

In the wake of the bombing, each of CSIS and the RCMP became fixated on a restrictive understanding of its own mandate, to the detriment of a co-ordinated effort to investigate the bombing. CSIS's focus on keeping its intelligence out of the judicial process led to the loss of important evidence and needlessly complicated the Reyat and Air India prosecutions. The RCMP's unimaginative approach to the investigation, as well as its dysfunctional focus on self-justification and on the pursuit of ready "evidence," led to the premature dismissal of potential leads, compromised the utility of human sources, and drove a further unnecessary wedge between it and CSIS.

It is important to note that, the story of the investigation of the Air India bombing demonstrates that the problems that plagued the relationship between CSIS and the RCMP were not simply the result of misunderstandings or personality conflicts. They were primarily the result of each agency's principled but overly narrow focus on its own mandate.

There is no doubt that, on both a personal and an organizational level, relations between CSIS and the RCMP are more cordial at present. The channels of communication are more open and a measure of coordination in the area of "deconfliction" has been achieved. Nevertheless, on an operational level, the central issues have not been resolved. The structures adopted by CSIS and the RCMP, which seek to minimize the passage of CSIS information to the RCMP, exacerbate, rather than relieve, the problem. They continue to deprive the RCMP of CSIS intelligence without, at the end of the day, protecting that intelligence from disclosure at trial. It follows that the resolution of issues related to cooperation cannot rely solely on improving personal relationships.

Volume Three is directed at providing better resolutions for the remaining real problems in cooperation as they manifest themselves in the criminal trial process.

The Future

Peter Archambault, in a paper written for the Research Studies volumes of the Report, contends that the terrorism of 1985 is not necessarily the same as the terrorism of today[3]. He accurately depicts it as continuously changing. This view is supported by the growing variety of "home-grown" terrorist cells emerging in the Western World. While this subject is not included in the Terms of Reference, it became evident during the Commission's work that this particular sort of terrorism represents an increasing threat to Canada; media and government commentary from the United States and Britain reflect considerable concern with the same phenomenon. Nevertheless, despite these evolutionary changes to terrorism, the Air India narrative continues to raise issues and to give illustrative

---

3 Peter M. Archambault, "Context is Everything: The Air India Bombing, 9/11 and the Limits of Analogy" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation.

examples that are entirely sufficient to provide a comprehensive springboard for a discussion of the policy issues assigned to this Commission.

Important as it is to establish the facts about what happened in the past, it is equally necessary to look ahead. The Commission's mandate requires recommendations for future actions dealing with aviation security, with the prevention or limiting of terrorism financing, and with the criminal prosecution of terrorism; especially as it relates to the use of intelligence as evidence.

The issues to be tackled are complex. For purposes of this introduction, it will suffice to provide a few comments that will help orient the reader to the thematic presentation in this volume and the detailed discussions in the Report itself.

The actual recommendations of the Commission with regard to these issues are to be found at the end of this volume.

1.6 Aviation Security

Because of the high propaganda value offered by a successful terrorist attack on an aircraft, civil aviation will continue to present an appealing target for terrorists. As a consequence, Canada cannot afford a return to the complacency that marked its approach to civil aviation security in 1985. Just as importantly, specific steps must finally be taken to close gaps that have been known to exist for decades. Modern civil aviation security regimes rely on the concept of mutually reinforcing layers. At present, some of the layers in the Canadian regime are too thin, or too widely-spaced, with insufficient overlap.

History has taught that terrorists continually probe security systems, looking for gaps and weaknesses. Airport security and air cargo are obvious deficiencies in Canada's current civil aviation security regime. Airports provide a means of introducing bombs and hijackers onto aircraft and are themselves targets of opportunity. Yet, perimeter security is lax and access to airside and restricted areas is poorly controlled. The majority (i.e., at least 70 per cent) of air cargo in Canada is transported on passenger flights, but, in stark contrast to the multi-layered approach currently used to screen passengers and their baggage, air cargo is not routinely searched, X-rayed, or subjected to adequate screening measures. The time has come to address these deficiencies.

Paradoxically, the emphasis on screening passengers and their baggage – a focus that has resulted from the Air India bombing and the 9/11 attacks – has contributed to the perpetuation of these deficiencies by drawing resources away from other aspects of the Canadian aviation security regime. To its credit, the current Government has moved to address this problem, but much more will be required to ensure that civil aviation security becomes, and remains, a national security priority.

In addition to other recommendations, the Commission has recommended periodic reviews of Canada's aviation security regime so as to guard against

complacency, ensure compliance with international obligations, and assure adequate funding for the system.

1.7 Terrorism and Criminal Prosecution

Society has an interest in the effective prosecution of crime, and terrorism is clearly a crime. Terrorism, however, is not simply a crime. It is also an existential threat to the societies it attacks, and Government has a legitimate interest in preventing terrorism, above and beyond that of punishing terrorists as criminals.

The collection and analysis of intelligence is a central resource in responding to the threat of terrorism and in preventing terrorist acts. The current reality is that CSIS will almost always be the first repository of information about terrorist offences that may ultimately be dealt with in a court of law. Complex and vexing problems can arise when the requirements of the criminal justice system for openness, as part of its constitutional commitment to a fair trial, are confronted by the need for intelligence information to be kept secret for purposes of protecting national security.

The approach recommended by the Commission is for both the criminal justice system and the intelligence community to review their procedures and to practise self-discipline so as to minimize the occasions when there is a true conflict between the need to disclose and the need to keep a secret. Where the conflict cannot be avoided, the key to a proper resolution is not to be found in some abstract rule or guideline, but rather in having in place a decision-maker sufficiently removed from the immediate interests of the contending institutions to be able to make a decision in the public interest.

Volume Three follows this approach through a number of potential decision points and provides specific recommendations for improvements to help the intelligence community, the police and the criminal justice system deal with the challenges associated with terrorism prosecutions.

These recommendations include an expanded mandate for the National Security Advisor to the Prime Minister, the creation of a new position of Director of Terrorism Prosecutions within the Department of Justice and a reconfiguration of decision-making procedures related to witness protection issues in terrorism investigations and prosecutions. They also include a recommendation that, in the context of terrorism prosecutions, the responsibility for reconciling the competing claims of disclosure to ensure a fair trial and secrecy to protect national security should be consolidated and assigned to the trial judge, rather than, as is now the case, being bifurcated between the trial court and the Federal Court of Canada.

In addition, in light of all the evidence before it, the Commission believes that the RCMP is not properly structured to deal with the unique challenges of terrorism investigations. There is merit in considering structural changes to

allow for a greater degree of specialization and for a more concentrated focus on investigating and supporting the prosecution of national security offences. This may mean divesting the RCMP of its contract policing duties so as to simplify lines of communication and to clarify the national dimensions of its mandate as a pan-Canadian police force.

1.8 Terrorist Financing

Canada is under a number of international obligations concerning the detection and prevention of terrorism financing. Compliance with these obligations is extremely important, and there is room for improvement by Canadian authorities in this regard.

Most of the current mechanisms that governments have in place to deal with terrorism financing are based on a money laundering model. While there are good reasons for this approach, the analogy is not perfect and therefore the model is of limited usefulness. Money laundering, driven by profit, involves the transfer, of, usually, large sums of money gleaned from criminal or other illicit activities, with the intention of concealing those criminal origins. Terrorism financing, driven by ideology, involves the transfer, often of small sums of money, whose origin may well be perfectly legitimate, with the intention of concealing their ultimate intended use for the illicit and criminal purposes of terrorism. Stopping this flow will require additional creative approaches.

The Regulatory authorities currently dealing with terrorism financing follow policies and procedures whose origins are in the oversight and enforcement of the *Income Tax Act* and which are subject to strict requirements of confidentiality. The analogy is not perfect in this respect either, and consideration should be given to developing means to allow for a more analytic, "intelligence-oriented" approach that may require further loosening of restrictions on the information that can be shared, while continuing to respect the legitimate privacy rights of Canadians.

1.9 The Government, the Families, and the Role of a Public Inquiry

In the days immediately following the bombing of Flight 182, responsibility for coordinating the Government response was transferred from the public service and was assigned to a representative of the Prime Minister's Office.

The Government response soon became focused on public relations and on defending the reputation of the Government and its agencies in order to protect them from criticism and from any possible finding of liability or any obligation to compensate the families of the victims.

Instructions were issued to avoid referring to the crash as a "bombing." Canada took the singular position at the Coroner's Inquest in Ireland that there was no evidence of a bomb aboard Flight 182 and, based on this argument, the

Coroner instructed the jury that they should make no recommendations about the cause of the crash. The Canadian Aviation Safety Board was prevented from filing a separate brief with the Kirpal Commission, which had been established by the Government of India to investigate the crash. The purpose was to ensure a consistent and positive portrayal of the safety and security arrangements that were in place in Canada at the time of the bombing. In the result, Canada succeeded in keeping any conclusions about responsibility for the crash out of the Kirpal Report.

Issues of civil liability loomed large. The Government denied any obligation to compensate the families of the victims and treated the families as adversaries. The defensiveness increased once the families brought an action for compensation. The civil claim was settled by hard bargaining at an early stage, before the Government was obliged to disclose its documents. Thus key information, like the existence of the June 1st Telex, was not disclosed to the families. Even after the civil litigation was settled, the Government resisted disclosure of information about the bombing on the grounds that the police investigation was ongoing. When the authorities did disclose potentially embarrassing information, it was mainly as a result of a leak to the press. The police did not meet with the families of the victims as a group until 1995, and CSIS would not meet with them until 2006.

In response to calls by the families for a review or public inquiry, the Government consistently refused, citing the ongoing investigation. When in 1991, SIRC finally conducted a review of CSIS's activities in relation to the Air India bombing, including the erasure of the Parmar tapes, the Government responded by putting together a coordinating committee in order to ensure consistency in the submissions by government agencies. The RCMP chose to accentuate the positive and submitted an 11-page, double-spaced brief whose major message was that any problems in cooperation between CSIS and the RCMP were in the past and that CSIS's actions had not hindered the police investigation. This was done despite the existence of internal RCMP documents which portrayed a very different situation. SIRC's report reflected this manufactured message.

When the RCMP investigation hit a 'dead end' in the early-to-mid 1990s, consideration was given to shutting down the investigation. There were concerns in Government that, once the investigation was at an end, a public inquiry would have to be struck. The RCMP decided to give the investigation one last best attempt. For the next 10 years, the need to protect the ongoing investigation and then, after that, the integrity of the trial process, were cited as reasons to refuse an inquiry.

In the aftermath of the 2005 acquittals, there were renewed calls for a public inquiry. Despite growing public pressure, there were still arguments made, including by Ministers of the Crown, that nothing could be learned from a public inquiry and that the trial had canvassed all the issues.

In fact, nothing could have been further from the truth.

1.9.1 The Present Inquiry

Individuals and institutions who are called before an inquiry are entitled to the assistance of counsel to help them protect their reputations. Government should pay for this representation, but its interests in an inquiry are quite different.

It is Government that calls the inquiry and, as a result, its goal must be to get the most accurate, impartial and useful answers to its questions and to let the chips fall where they may. In this Inquiry, the Department of Justice, which is the Government's law firm, was retained to represent the reputation and interests of all government employees and institutions. An arrangement of this type raises a potential conflict because of the differing goals of the Government calling the Inquiry and of the government witnesses and institutions wanting to defend their reputation.

Even with the best of intentions and the utmost in probity, there is danger that one set of lawyers will act like the coordinating committee that oversaw the submissions of the various government agencies to the 1991 SIRC Review.

This Inquiry was called in response to the families' decades-long quest for meaningful answers, as undeniable deficiencies in the response of some government agencies have trickled out in reviews and prosecutions over the years. The evidence heard in the Inquiry left no doubt that many government witnesses unequivocally felt the response of certain government agencies was problematic or deficient.

Given that reality, it was disturbing that the Department of Justice, the lawyer for the Government that called this Inquiry, was put in the position of making submissions on behalf of its clients to the effect that there is no basis for any criticism of the actions of *any* government agency in connection with the investigation of the bombing of Flight 182. And further, it argued that *no* changes are needed in current policies and procedures dealing with interagency cooperation, aviation security, terrorism financing or the competing demands of security intelligence and the criminal justice system. In essence, the Department of Justice ended up taking one of two closely related, but equally unhelpful, positions: either that of claiming that there was no reason for this inquiry to have been called in the first place, or that of saying, in effect, "It wasn't broken, but we fixed it anyway."

That is the unfortunate result of the Government's multiple parties trying to "speak with one voice." Government ends up denying everything and saying nothing constructive. More than that is owed to families of the victims and the rest of the Canadian public.

The agencies of the Government have a duty to provide a commission of inquiry with full and frank disclosure of all relevant information in as timely a manner as possible. The "public" dimension of a public inquiry also requires that as much of this information as possible be made available in a form that can be disclosed to the public.

Claims to exemption from public disclosure, whether on the basis of National Security Confidentiality (NSC), the requirements of an ongoing criminal investigation or some other privilege or exception, must be carefully weighed before they are asserted. These should not be blanket claims. In each case a pragmatic assessment needs to be made as to the true harm disclosure is likely to cause as against the benefit of allowing the Commission to carry on its work in public.

The performance at this Inquiry in this regard by each of the relevant government agencies was mixed. The agencies initially took positions as to what should be protected from disclosure on the basis of National Security Confidentiality that would have made it impossible for this Inquiry to be conducted in public. It was only after the Prime Minister intervened directly that there was movement from this position by the agencies.

CSIS was over-zealous in its claims of NSC. This, combined with the Service's tendency to answer only the precise question asked and nothing more, made telling the CSIS story more difficult than necessary. Transport Canada's documentary disclosure was tardy and disorganized, making it difficult to deal with a number of aviation security issues in the public hearings. These difficulties were compounded by Transport Canada taking unhelpful, and ultimately untenable, positions on what could be disclosed to the public – positions that seemed aimed more at preventing embarrassment to the agency than at protecting any realistic interest in secrecy.

The conduct of the RCMP on disclosure issues was especially troubling to the Commission. There were several instances in which the Commission was discouraged from pursuing certain areas of investigation on a doubtful assertion of the requirements of "the ongoing investigation," assertions at times based on investigative initiatives that were revived by the RCMP after the Commission began making enquiries.

One incident in particular was especially troubling. "Mr. G," a person with potential knowledge of matters relating to the bombing of Flight 182, told the RCMP during the currency of the hearings that he wished to speak to the Commission and to testify. Rather than inform the Commission of the approach by this witness, the RCMP instead used the fact that Mr. G had contacted the RCMP as the basis for demanding further redaction of previously cleared documents, asserting that this was necessary in order to protect the ongoing criminal investigation. Even after the Commission by chance discovered Mr. G's attempts to make contact, the RCMP did not confirm this fact until after the close of the hearings, months after being asked directly by the Commission. The RCMP then continued to assert the need to protect the integrity of its ongoing investigation hoping to discourage the Commission from pursuing the matter, even after it had interviewed Mr. G and dismissed the utility of his information for police purposes.

1.9.2 Racism

A suggestion was made during the hearings that the Government's attitude to the bombing and its treatment of the families of the victims was a manifestation of "racism," though not perhaps of a conscious sort.

The Commission finds that the term "racism" is not helpful for purposes of understanding the Government response. "Racism" carries with it so many connotations of bigotry and intolerance that even the most careful definition that purports to focus on effects rather than on intent ends up generating a great deal more heat than light. This was amply illustrated on the hearing date devoted to evidence regarding this issue.

While the Commission does not feel that the term "racism" is helpful, it is also understandable that the callous attitude by the Government of Canada to the families of the victims might lead them to wonder whether a similar response would have been forthcoming had the overwhelming majority of the victims of the bombing been Canadians who were white. The Commission concludes that both the Government and the Canadian public were slow to recognize the bombing of Flight 182 as a Canadian issue. This reaction was no doubt associated with the fact that the supposed motive for the bombing was tied to alleged grievances rooted in India and Indian politics. Nevertheless, the fact that the plot was hatched and executed in Canada and that the majority of victims were Canadian citizens did not seem to have made a sufficient impression to weave this event into our shared national experience. The Commission is hopeful that its work will serve to correct that wrong.

1.9.3 Treatment of the Families

The families of the victims of the bombing were poorly treated by their Government. For the longest period of time the Government seemed dedicated to self justification and denial of fault that led it to cast a blind eye and a deaf ear to the suffering and the needs of the families.

The Government was too preoccupied with its international reputation to appreciate its obligations to the families of the victims. It was so keen on debunking any notion that the bombing was tied to deficiencies in Canadian safety and security that it alienated the very people who deserved support and empathy: the families of the victims.

It is hard to believe that a desire to avoid civil liability to the families of the victims – for an amount that, in the big picture, would not have constituted a rounding error in the budget of any of the Canadian agencies involved – would have motivated the Government of Canada to turn its back on the victims for so long.

In stark contrast to the compassion shown by the Government of the United States to the families of the victims of the 9/11 terrorist attacks, for all too long the

Government of Canada treated the families of the victims of the terrorist attack on Flight 182 as adversaries. The nadir of this attitude was displayed when the families' requests for financial assistance were met by the Government's callous advice to seek help from the welfare system.

Even after the modest settlement of the civil litigation, a settlement which, ironically, prevented the families from receiving disclosure from Government of the extent of the deficiencies in the pre-bombing period, the Government was slow to recognize any duty towards the victims or their families.

A notable exception to this past neglect is to be found in the elaborate and effective mechanisms implemented by the post-1995 RCMP Air India Task Force, which made it possible for them to liaise with, understand and provide support to the families of the victims over the course of the Air India prosecution.

The establishment of the present Commission of Inquiry is a further positive development, but the fact remains that, for over two decades, the Government of Canada and its agencies stood adamantly opposed to any public review.

The Government and its agencies have the right to defend themselves and to put their best foot forward, in the context of civil litigation and in public inquiries such as this one. However, the Government was indiscriminate in its denials, doggedly denying all potentially unflattering facts, even some that had been uncontrovertibly shown to be true. As well, the Government's constant over-claiming of privilege and its continued withholding of information have had a painfully negative impact on the vulnerable families of the victims of this immense tragedy.

Whatever "truth and reconciliation" may be generated by the present Inquiry, it remains the case that, long after the settlement of the civil litigation, important information continued to be withheld from the families. It took a decade for the RCMP, and two decades for CSIS, to appreciate the need to meet with the families.

1.10 Doing More for the Families

Although condolences to the families of the victims have been frequent and free-flowing during the course of this Inquiry, no one on behalf of the Government of Canada or its agencies has thought it appropriate to offer an apology. The record before the Commission demonstrates that there is a great deal to apologize for.

Some steps have been taken to correct the neglect of the past.

The erection of memorials and the annual ceremonies of commemoration on June 23 are excellent and tangible demonstrations of Canada's attempts to integrate the bombing of Flight 182 into Canadian history and consciousness.

The Commission believes that there is more that could be done.

As discussed in the Volume Five, the funding of an academic institute for the study of terrorism, – possibly to be called the "Kanishka Centre" to commemorate the name of the aircraft that was bombed on June 23, 1985 – could be an important step toward preventing future terrorist attacks while honouring the memory of those who perished in the bombing.

The Commission also believes, however, that there would be great merit in a demonstration of solicitude by the current Government, even at this late date, for the families of the victims of the bombing. There is nothing in the Terms of Reference to prevent the Commission from asking that the Government consider a one-time *ex gratia* payment to family members of the victims of Flight 182. To that end, an arm's-length independent body should be constituted to recommend an appropriate amount, as well as a formula for its distribution, and should remain in existence to oversee the payment process. Providing an *ex gratia* payment will go a long way to alleviating what is now over twenty years of alienation for those Canadian families.

The mandate of this Commission expires with the publication of the Report and its Recommendations. The families of the victims and the Canadian public will want to know whether the Recommendations have been accepted and how they have been implemented. The Government should provide a Report, perhaps through the Office of the Auditor General, on which Recommendations have been implemented and which have been rejected.

VOLUME ONE
THE OVERVIEW

CHAPTER II: THE INQUIRY PROCESS

2.0 Introduction

Commencing more than 20 years after the events under consideration took place and mandated to examine a broad range of factual and policy issues, this Inquiry was faced with significant challenges from the outset. As the work unfolded, further specific obstacles to the expeditious conduct of the Inquiry appeared. Most notable among these was the need to address National Security Confidentiality (NSC) issues. This chapter describes how the Commission approached its mandate, and discusses some of the procedures used to ensure that the Inquiry could proceed as efficiently as possible. The chapter also reviews the various special challenges encountered, many of which have contributed to extending the time and resources necessary to complete the Inquiry's mandated work.

2.1 Outline of the Inquiry Process

2.1.1 Mandate and Initial Process

By Order in Council dated May 1, 2006,[1] the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 was established pursuant to Part I of the *Inquiries Act*.[2] The Honorable Bob Rae, who had been appointed in 2005 to provide independent advice to the then Minister of Public Safety and Emergency Preparedness, had previously concluded that, in spite of the passage of 20 years since the terrorist attack on Flight 182, outstanding questions of public interest still required answers.[3] The Terms of Reference for this Inquiry require the Commission to make findings and recommendations with respect to a broad range of issues arising out of the Air India investigation and prosecution, including issues of threat assessment, aviation security, interagency cooperation, terrorist financing, witness protection, the relation between security intelligence and evidence, as well as the unique challenges presented by the prosecution of terrorism cases.[4]

---

1 P.C. 2006-293 (referred to here as the "Terms of Reference").

2 R.S.C. 1985, c. I-11.

3 See *Lessons to be Learned: The Report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182* (Ottawa: Air India Review Secretariat, 2005).

4 See P.C. 2006-293, para. (b).

On June 21, 2006, an initial session of the Commission was convened at which a public opening statement was made on behalf of the Commission addressing procedural matters and setting out some of the principles which would guide the conduct of the Inquiry. The statement expressed the Commissioner's intention to conduct a thorough investigation in compliance with the Terms of Reference and the legal requirement to act fairly.[5]

In June and July 2006, *Rules of Procedure and Practice* were adopted[6] and the Commission received 21 applications for Standing. On August 9, 2006, a ruling was issued granting 18 of the applications.[7] Two types of standing were granted to the successful applicants: Party Standing and Intervenor Standing. Party Standing, the more extensive type reserved for those directly and substantially affected by the mandate of the Inquiry, was granted to a total of eight individuals and organizations, including individual family members of the victims of Air India Flight 182 and organizations representing family members, the Attorney General of Canada (AGC) on behalf of the Government of Canada and all affected departments and agencies, as well as Air India. Family members and organizations representing them were divided into three main groupings for purposes of representation: the Air India Victims Families Association (AIVFA), representing a large group of family members residing in North America, Lata Pada and other individuals aligned with her, mostly residing in North America but not members of AIVFA, and a grouping including the Air India Cabin Crew Association (AICCA), the Family Members of the Crew Member Victims of Air India Flight 182 and India Nationals (FMCMV/IN), as well as individual family members residing in India. Each group was encouraged to cooperate with other groups to the extent possible to avoid repetition during the Inquiry hearings. This was accomplished successfully through a division of labour among counsel representing the three groupings, which ensured that specific areas of evidence were not canvassed separately where the Parties' interests did not require it. On August 9, 2006, Intervenor Standing was granted to a total of 10 organizations and individuals with interests and perspectives relating to the Commission's mandate. As a result of further applications presented during the following months, three additional organizations received Intervenor Standing and one additional individual received Party Standing.[8] Intervenors included a number of organizations representing civil liberty and Canadian democracy interests, as well as organizations representing the legal profession and law enforcement.

Individuals and organizations with Party Standing were represented in the Inquiry hearings and participated by cross-examining witnesses and making submissions on a regular basis. Intervenors had opportunities to participate by presenting written submissions and, in some cases, making oral opening statements.

---

5 Opening statement of the Commissioner, Transcripts, June 21, 2006, pp. 8, 10.

6 See *Rules of Procedure and Practice* for the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (revised July 17, 2006).

7 August 9, 2006 *Ruling on Standing* in Annex A of this Volume.

8 *Rulings on Standing* dated August 23, 2006, November 1, 2006, March 14, 2007 and May 11, 2007 included in Annex A of this Volume.

On October 12, 2007, one of the Intervenors, the World Sikh Organization (WSO) applied for broader standing, including the right to cross-examine witnesses and to receive notices and documents, and asked that Commission counsel be compelled to call a number of witnesses.[9] On October 29, 2007, the Commissioner granted expanded Intervenor status to the WSO, allowing it to make submissions on all Terms of Reference, but noted that the right to cross-examine witnesses belonged to Parties alone and that the witnesses the WSO wanted called, with one exception, were either already scheduled to testify or did not have evidence relevant to the Terms of Reference.[10] Not satisfied with this ruling, the WSO raised numerous complaints throughout the remainder of the Inquiry and used its Final Submissions, filed on January 31, 2008, to challenge the Commissioner's decisions and even to attempt to circumvent prior rulings by appending documents and referring to "facts" which had not been admitted into evidence and which, in any event, contributed little to matters relevant to the Terms of Reference.[11]

Counsel for the WSO had an important role to play with respect to the reputational interests of the Sikh community. Instead, they expended considerable time, resources, and energy seeking to advance a number of peripheral issues beyond the jurisdiction of the Commission through repeated motions to tender evidence intended to suggest that the Government of India was involved in the bombing of Air India Flight 182. It is regrettable that the WSO missed the opportunity to make a more meaningful contribution to the Inquiry with regard to promoting Sikh reputational interests. Fortunately, those interests were well protected by the evidence brought forward at the Inquiry, which has amply demonstrated that Sikhs in Canada are law-abiding, peaceful, and outraged by the terrorist attacks on Flight 182 and at Narita.

Commission counsel, charged with representing the interests of the Canadian public at the Inquiry, were automatically a Party before the Commission.[12] All Commission counsel were appointed by the Commissioner to assist him in carrying out his mandate. They were responsible for bringing all matters relevant to the Terms of Reference to the Commissioner's attention. Their role was to assist the Commissioner in a non-partisan and non-adversarial manner throughout the Inquiry.[13] To this end, Commission counsel reviewed documents, interviewed witnesses and led the evidence in the Inquiry hearings.

The Commissioner was authorized by the Terms of Reference to recommend that funding be provided to ensure the appropriate participation of the families of

---

9 See *WSO Application for Broader Standing*, October 12, 2007 and *WSO Applications to Call Zuhair Kashmeri, Gary Bass, David Kilgour and Gian Singh Sandhu as Witnesses*, October 12, 2007 in Annex A of this Volume.

10 See *Ruling on Standing* and *Ruling on Application to Call Certain Witnesses*, October 29, 2007 in Annex A of this Volume. One of the witnesses proposed by the WSO was called by Commission counsel on December 7, 2007, but the testimony had to be restricted for relevance and because of civil litigation issues.

11 See *WSO Final Submissions*, January 31, 2008.

12 See *Rules of Procedure and Practice*, Rule 2(c).

13 Ontario, *Report of the Walkerton Commission of Inquiry, Part One* (Toronto: Queen's Printer for Ontario, 2002), p. 479 [*Walkerton Report*].

the victims and of any Party granted standing.[14] Recommendations were made to provide funding for counsel representing family members organizations or groups, as well as some of the Intervenors. Those recommendations were accepted by the Government of Canada.

As set out in the *Rules of Procedure and Practice*, the Inquiry hearings were divided into two separate but interrelated stages. Stage 1, which proceeded during the fall of 2006, with one additional witness heard in June 2007, involved the voluntary testimony of family members of the victims of the bombing of Air India Flight 182, who are themselves victims of terrorism. Many family members chose to be heard in the Inquiry hearings to share memories of their lost loved ones, as well as to describe the impact of the bombing and share expectations for the Commission. Printed, audio and video materials were submitted. During Stage 1, the Commission also heard evidence from individuals who were involved in the first response following the explosion. A report entitled *The Families Remember*[15] was released in December 2007, while the Inquiry continued to receive evidence with respect to Stage 2 of the hearings. This first report attempted to record the human toll of the Air India bombing. It was felt that the families had already waited too long to have their stories told and that there was no reason to wait for the entire Inquiry to be complete prior to the release of this first report. Stage 2 of the Inquiry proceeded from November 6, 2006 to December 13, 2007[16] with an inquiry into the matters set out in clauses (b)(i)-(vii) of the Terms of Reference.

2.1.2 Document Collection Process

In July 2006, the Commission issued its first requests for documents and information relevant to the Commission's mandate in the possession of the government departments and agencies involved, beginning with a request dated July 12, 2006, for all documents "relevant to the mandate of the Commission as set out in the Commission's Terms of Reference." Over the ensuing months, numerous additional requests followed as existing documentation was reviewed and new facts learned through the witness interviews and testimony.

New documents were, accordingly, received by the Commission on a continuous basis throughout the proceedings. Even after the conclusion of the hearings, new documents continued to be delivered, sometimes in response to requests from Commission counsel for further information, sometimes at the Government's own instance. A total of 17,692 documents consisting of tens of thousands of pages were provided via a secure electronic network which allowed the Commission to review and organize the materials. In addition, the Commission was provided with access to a portion of the RCMP database on the Air India investigation, containing countless documents with a total number

---

14 P.C. 2006-293, paras. (g) and (i).

15 The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *The Families Remember* (Ottawa: Public Works and Government Services Canada, December 2007).

16 Two additional hearing days were also held in February 2008.

of pages ranging in the millions.[17] Thousands of additional pages of hard copy documents were also obtained and further access was provided to materials which were made available for review on Government premises.

Although document collection did not always proceed smoothly or without incident, ultimately sufficient documentation was identified and made available to the Commission to allow it to discharge the mandate set out in the Terms of Reference. The Attorney General of Canada certified that it was satisfied that the Government and its agents, servants, agencies and departments had diligently searched for and produced to the Commission documents "potentially relevant" to the Commission's Terms of Reference as well as documents responding to the Commission's subsequent document requests.

2.1.3 National Security Confidentiality Claims and Redaction of Documents

All documents received by the Commission from the Government, except documents for which solicitor-client privilege or Cabinet confidence was claimed, were initially provided to the Commission with no deletions or redactions, regardless of any National Security Confidentiality (NSC) claims asserted or to be asserted by the Government.[18] All documents were handled by the Commission in accordance with their security classification.

Eventually, the Government asserted NSC claims and other privilege claims over a large portion of the documents initially provided to the Commission. The claims were made in cases where the Government took the position that the disclosure of information contained in the documents would be injurious to international relations, national defence or national security, or that it could identify confidential sources of information or compromise ongoing investigations.[19] A special process was agreed upon to enable the Government to notify the Commission of the exact documents and extracts over which it intended to assert NSC claims. Commission counsel were required to identify, after a first review of the documents provided by the Government, the documents they anticipated would be entered into evidence or be disclosed to the Parties in advance of the hearings. Lists of such documents then had to be provided to counsel for the Government in the form of "redaction requests". The Government subsequently provided redacted versions of the documents, where all information over which NSC claims were asserted was blacked out.[20] Commission counsel continued to have access to uncensored versions of all

17 Statement by Barney Brucker, Transcripts, vol. 19, March 9, 2007, p. 1770.

18 Where solicitor-client privilege or Cabinet confidence was claimed, the documents were generally provided to the Commission with the portions over which privilege was claimed already deleted. Where the privilege was claimed over entire documents, the documents were not provided to the Commission, but the Commission was advised of their existence upon request.

19 For present purposes, all Government privilege claims (except solicitor-client and Cabinet confidence which involved a different procedure) will be collectively referred to as NSC claims as the same procedure was followed with respect to all such claims in the context of this Inquiry.

20 A general description of this process was provided in the opening statement to Stage 2 of the hearings by Mark J. Freiman, Lead Commission Counsel, Transcripts, vol. 12, November 6, 2006, pp. 1045-1046.

documents, but only the redacted versions could be disclosed to the Parties and entered into evidence.

In September 2006, the Commission began to receive Government documents in response to its July 2006 and subsequent requests. Approximately 4,500 documents were initially received and the documentary review and redaction requests process began. Meanwhile, as the document collection process continued, more new documents were provided to the Commission in response to prior and new requests. Because a vetting process had already commenced within Government, it was possible in October 2006 for the Commission to provide to the Parties, in redacted form, approximately 1500 documents identified as essential by the Government. Commission counsel progressively sent lists of additional documents requested for redaction to the Government as the documentary review continued, but it was not until December 2006 that the next installment of redacted documents was received. Because of this ongoing process, it was not possible to begin with the Stage 2 hearings in October 2006 as initially planned.[21] At the time, the Commission was still receiving new materials and, most importantly, the process of identifying documents and receiving redacted versions for purposes of disclosure to the Parties and production before the Commission had not progressed sufficiently.

Although it was planned to commence hearing Stage 2 evidence in November 2006, that timetable also proved impossible to meet, as a sufficient number of redacted documents was still not available.[22] This was in large part caused by the nature of the document collection process which required the identification, disclosure and review of documents from several different agencies, covering a period of time ranging over many years. Further, the document collection and redaction process involved electronic versions of documents, since the Terms of Reference required the Commission to process documents using the automated litigation support program prescribed by the Attorney General of Canada.[23] As a result, the process was highly dependent on technology. Unfortunately, several weeks' worth of the Commission's work in processing documents was lost in early November as a result of a technical glitch in the Government's uploading of new documents to the Commission's server.[24] In general, it was difficult for the Government to provide redacted versions of documents within short time frames given its process of extensive internal reviews involving different agencies and departments. It was also necessary to allow counsel for the Parties before the Inquiry sufficient time to review the documents to enable them to contribute to the hearings in a meaningful way. This could not be done until redacted versions of the documents were available for disclosure to the Parties' counsel. The hearings were therefore adjourned to February 2007 in the hope that this would allow sufficient time for this process to be completed.

---

21 Statement by the Commissioner, Transcripts, vol. 11, October 13, 2006, pp. 1041-1042.

22 See, generally, statements by Commission counsel, Government counsel and counsel for the families: Transcripts, vol. 12, November 6, 2006, pp. 1044-1051. Evidence about the Canadian consular response following the Air India bombing was nevertheless heard during the week of November 6, 2006.

23 P.C. 2006-293. para. (k).

24 Opening statement by Mark J. Freiman, Transcripts, vol. 12, November 6, 2006, pp. 1046-1047.

Unfortunately, the Stage 2 hearings could still not proceed as planned when the Commission hearings reconvened in February. At that point, a large number of redacted documents had been provided by the Government, but the extent of the proposed NSC claims advanced by the Government made the holding of public hearings impossible. The proposed redactions essentially made the documents meaningless, with too much of the information remaining censored and unavailable to counsel for the families and to the public. Under the circumstances, a meaningful discussion of the factual issues could not have taken place, since even the most basic facts and issues could not have been dealt with in public. A decision was made that resolution of this issue would require reassessment by Government of its position, rather than resorting to *in camera* hearings, either to hear the evidence on the merits or to rule on the justification for the proposed redactions. Since rulings would have been subject to judicial review, the result would inevitably have been long and complex judicial proceedings that would essentially have made the Inquiry "…disappear in the quicksand of bureaucracy."[25]

The Government was asked to reassess the proposed NSC claims before the Commissioner reported to the Prime Minister on the feasibility of carrying out the Inquiry's mandate.[26] Counsel for the Government agreed to work with Commission counsel to review the redactions and determine whether sufficient unredacted documentation could be made available to enable meaningful public hearings to proceed.[27] A new process was devised to provide the Government with an opportunity to reassess its NSC claims. Commission counsel agreed to review all of the documents initially provided by the Government in redacted form and to make a selection of the most important documents and information. To assist the Government, specific extracts of the documents were also identified. The Commission provided the Government with "redaction reconsideration requests" identifying the document extracts, and the Government proceeded to reassess its NSC claims.[28] New versions of the documents were eventually returned with significantly fewer redactions. The new versions were reviewed again by Commission counsel and any additional issues were brought to the Government's attention through "subsequent redaction reconsideration requests" specifically identifying the documents and extracts involved and triggering a new Government examination of NSC claims.

It was hoped that Stage 2 hearings could finally proceed in March 2007. However, the new redaction reconsideration process proved to be equally as time-consuming as the initial redaction process. It required Commission counsel to review for the second and third time a large numbers of documents in order to make the best selection possible and to enable the Government to reassess its claims. The process also placed considerable strain on the Government officials involved, and their ability to provide documents with revised redactions in an

25 Opening statement by the Commissioner, Transcripts, vol. 15, February 19, 2007, p. 1371.
26 Opening statement by the Commissioner, Transcripts, vol. 15, February 19, 2007, pp. 1370-1371.
27 Opening remarks by Barney Brucker, Transcripts, vol. 19, February 19, 2007, p. 1377.
28 See, generally, Statement by Barney Brucker, counsel for the Government, explaining the process: Transcripts, vol. 16, March 5, 2007, pp. 1414-1415.

expeditious manner was dependent on available resources. The Commission was advised by counsel for the Government in early March 2007 that, despite their best efforts, the reconsideration of NSC claims was not yet complete.[29] A sufficient amount of information could not yet be made available to counsel for the Parties to allow them to prepare and contribute in a meaningful way to the proceedings.[30]

As a result, it was only at the end of April 2007 that the Stage 2 hearings referring to the Government documents could finally proceed. Even then, the redaction reconsideration process was still ongoing with respect to documents relevant to the evidence anticipated to be heard in subsequent weeks. In fact, the process continued throughout, and even after the conclusion of the hearings. Documents continued to be received as a result of the ongoing disclosure requests. They were then redacted a first time by the Government following requests by Commission counsel, and then were often redacted a second and sometimes a third time following reconsideration requests. The Commission continued to receive documents from the Government after the conclusion of the hearings. When the documents were suitable for public release, they were produced to the Parties who were given the opportunity to make written submissions as to their contents.

2.1.4 Conduct of the Stage 2 Hearings

While most of the evidence relating to Stage 2 of the Inquiry could not be presented before April 30, 2007 because of the redaction reconsideration process, evidence respecting the Canadian consular response to the bombing, as well as some of the more general evidence respecting RCMP and CSIS structures and mandates, was nevertheless presented during seven hearing days in November 2006 and March 2007. The Stage 2 hearings then proceeded without interruption between April 30 and June 20, 2007 and between September 17 and December 13, 2007. Two additional days of hearings were held on February 14 and 15, 2008. During this period, a total of 85 days of hearings were held and 195 witnesses testified, some on more than one occasion.

In order to prepare the evidence to be presented in the Inquiry hearings, Commission counsel conducted numerous interviews with potential witnesses.[31] This process was necessary to identify the persons who had sufficient knowledge and memory of relevant facts and events. In most cases, the potential witnesses were present or former Government employees. Counsel for the Attorney General of Canada attended most of the interviews, including all interviews of current Government employees. Commission counsel then determined which individuals would be called as witnesses before the Commission and prepared

---

29 Statement by Barney Brucker, Transcripts, vol. 16, March 5, 2007, pp. 1414-1421.

30 As had been done during the week of November 6, 2006, the Commission nevertheless proceeded to hear some of the Stage 2 evidence which was not dependent on documentary production, this time with respect to the structure and mandates of CSIS and the RCMP.

31 See Rule 34 of the *Rules of Procedures and Practice*.

statements of the witnesses' anticipated evidence as well as lists of documents associated with the witnesses' testimony ("will say" statements).[32] Those statements were meant to assist the Parties, especially those whose counsel were not present during the interviews, to appreciate the nature of the anticipated evidence and to identify the relevant documents in order to prepare for any cross-examination. Pursuant to the Protocol for the Protection of Privileged Documents and Information between the Government and the Commission, in the case of all witnesses privy to Government documents produced to the Commission, the will say statements prepared by Commission counsel had to be submitted in advance to the Attorney General of Canada, who could then advise of any NSC claims that would be asserted by Government over the proposed evidence. Commission counsel were only permitted to disclose the will say statements to other Parties once they were advised by Government that no NSC issues were involved or once changes were made to remove any NSC concerns.

The Stage 2 hearings were divided into four different phases devoted to specific subject areas related to the Terms of Reference: law enforcement and intelligence response to Sikh terrorism, aviation security, terrorist financing, and terrorism and the justice system. The evidence heard included general descriptive, policy and expert evidence respecting the matters of inquiry, as well as detailed factual and historical evidence respecting specific actions taken in relation to the Air India bombing.

On May 1, 2007, a set of Evidence Binders containing most Government documents relevant to the historical aspects of the Commission's mandate was entered into evidence.[33] Throughout the remainder of the Inquiry, new documents were added to the Evidence Binders. As redactions were reassessed by Government, new versions of the existing documents were also added. At the end of the hearings, approximately 3,300 documents were entered as part of the Evidence Binders, many in more than one version as a result of the redaction reconsiderations. In addition, over 300 documents were entered as separate exhibits throughout the Stage 2 hearings, some simply as updates to the Evidence Binders, others containing many new separate documents. Further updates to the Evidence Binders and other documents, totaling approximately 230, were also entered after the conclusion of the hearings as a result of the continuing document production and redaction process. The limited number of documents entered, as compared to the volume of documentation obtained by the Commission in the document collection process, is a reflection of the selection that had to be made in the context of the NSC claims reconsideration process. Only documents considered essential to the Inquiry's mandate were entered into evidence.

---

32 See, generally, Rules 35 and 50 of the *Rules of Procedure and Practice*.
33 Exhibit P-101.

In February and March 2008, the Parties before the Inquiry provided Final Submissions in writing.[34] The submissions addressed the factual issues before the Commission in considerable detail, and provided suggestions of possible recommendations to avoid the recurrence of any deficiencies identified and to address the broader policy issues within the Commission's mandate. All Parties were provided with an opportunity to respond to the submissions presented by other Parties. Many of the Intervenors also provided written submissions focusing on specific areas of inquiry relevant to their expertise and experience, and also suggesting recommendations.

Commission counsel did not prepare written final submissions at the close of the Inquiry hearings in the same manner as Intervenors and Parties. Written submissions were filed by these groups to represent their particular interests and to advocate for specific recommendations. Since Commission counsel, like the Commissioner, were responsible for representing the interests of the Canadian public at large and not of any particular group, it would not have been appropriate for them to file submissions. Their role was rather to ensure that all relevant evidence was presented, that all sides were heard and that all relevant matters were considered.[35]

2.1.5 Section 13 Notices

The Commission issued notices in accordance with section 13 of the *Inquiries Act*[36] to those who might be the subject of findings of misconduct or unfavorable comments in the Commissioner's report. In the context of this Inquiry, such notices were, in the end, only issued to institutions and not to individuals. As required by law, the notices were issued confidentially. The institutional recipients of the notices were provided with an opportunity to be heard and to be represented by counsel in order to respond to any allegations of misconduct. In fact, all recipients had been entitled to participate fully in the Inquiry hearings and were represented by counsel throughout. They could cross-examine witnesses, suggest evidence to be presented by Commission counsel, apply to the Commissioner to present evidence not otherwise presented by Commission counsel, and make closing submissions. Commission counsel advise that no suggestion made by the recipients of the notices for evidence to be called was refused during the course of the Inquiry.

2.1.6 Inquiry Report

The purpose of this Report is to analyze the evidence heard in the public hearings with a view to making recommendations about the changes that can be made to avoid the pitfalls encountered in the Air India matter and to improve Canada's

---

34 Counsel for the Air India Victims' Families Association also presented oral submissions before the Inquiry: see Transcripts, vol. 97, February 15, 2008, pp. 12865-12898 (Closing submissions by Jacques Shore, Norman D. Boxall, Raj Anand and Richard Quance).

35 *Walkerton Report*, p. 479.

36 R.S.C. 1985, c. I-11.

ability to respond to the modern reality of terrorism. The recommendations are based on factual findings about what, if anything, went wrong in the investigation of Sikh terrorism and of the Air India bombing, and about the challenges that remain with respect to the response to modern terrorism more generally. Rather than chronologically summarizing the facts and evidence, the substantive issues as set out in the Terms of Reference are used as organizing principles to analyze the evidence and draw conclusions where appropriate.

The Report is based on the evidence presented in the public hearings and in the Commission dossiers. At times, the Commission has taken special measures to protect the identity of certain individuals, where it was felt that their safety could be jeopardized or where court ordered publication bans required it. In some cases, this was achieved by applying additional redactions to Government documents entered into evidence. In a limited number of instances involving less than 20 documents, this was accomplished by not entering into evidence some documents that had been returned by the Government in redacted form. In such cases, the Government quite appropriately refrained from making NSC claims as no national security issues were involved, but the disclosure of the documents, even if the Commission had applied additional redactions, could have jeopardized the safety of individuals. Where facts are described in the Report without reference being made to documents entered into evidence before the Commission, it is because the documents, though not subject to NSC claims, were part of the small number of documents held back to protect individual safety.

The findings of fact in the Report and the opinions expressed are not legal findings of responsibility. They are meant to describe for the public what happened as revealed by the evidence and what can be done to ensure that any such deficiencies do not recur. As mandated by the Terms of Reference, there are no conclusions or recommendations respecting the civil or criminal liability of any person or organization.[37] While, in some cases, the alleged actions or omissions of various individuals or organizations in connection both with the Air India bombing and its investigation had to be examined or mentioned, nothing in the Report should be interpreted as an indication that the Commission has come to any conclusions about the civil or criminal responsibility of anyone.

2.1.7 Research Papers

Fifteen research papers were written for the Commission. Research studies have long been an important part of the public inquiry process in Canada. For example, the McDonald Commission of Inquiry, which examined activities of the Royal Canadian Mounted Police (RCMP) and made recommendations that led to the creation of the Canadian Security Intelligence Service (CSIS) in 1984, issued

---

37 P.C. 2006-293, para. (p).

a number of research papers and monographs as part of its process.[38] Other commissions of inquiry have also undertaken ambitious research agendas.[39]

Research papers were particularly important, given the breadth of this Inquiry's mandate. A broad range of expertise drawn from a variety of academic disciplines was needed to address this mandate. The Commission was fortunate to be able to retain the majority of Canada's leading experts in many of these areas. The Commission was also able to retain a number of leading international experts to provide research of a more comparative nature. The comparative research was undertaken to determine if Canada could learn from the best practices of other democracies in many of the areas related to the Commission's mandate.

The research papers were written independently on the basis of available public sources. They were also written in a timely manner so that they could be made available to the Parties and Intervenors during the Commission's hearings. The researchers did not have available to them all the evidence that was called throughout the Inquiry. This allowed for the expeditious preparation of the papers. It also recognized that it was the mandate of the Commissioner, who presided over all the hearings, and not the researchers, to draw conclusions based on the evidence heard at the Inquiry. The recommendations of the independent researchers did not necessarily represent those of the Commission. Indeed, the papers were designed in part to formulate tentative proposals that could be tested and challenged by Parties and Intervenors at the Inquiry.

In almost every case, the experts who wrote the reports were called to testify in the Inquiry's proceedings with a preliminary version of their papers being disclosed in advance to the Parties. Such a process has not been the norm for commissions of inquiry. Nevertheless, it proved to be useful as a vehicle to test and challenge the ideas and proposals put forth by the researchers. There was also a concern that the Commissioner should be able to see the research produced for him challenged and defended in a public forum.

Canadian research into terrorism-related issues has generally been relatively sparse.[40] A decision was made to translate and publish the research studies and release them in four volumes with the Report. One of the functions of a public

---

38 For example, see the research studies published by the McDonald Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. J. Ll. J. Edwards, *Ministerial Responsibility for National Security as It Relates to the Offices of Prime Minister, Attorney General and Solicitor General of Canada* (Ottawa: Supply and Services Canada, 1980); C.E.S. Franks, *Parliament and Security Matters* (Ottawa: Supply and Services Canada, 1980); M.L. Friedland, *National Security: The Legal Dimensions* (Ottawa: Supply and Services, 1980).

39 Recent examples are The Commission of Inquiry into the Sponsorship Program and Advertising Activities (2006) and The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar. Among the series of background papers published by the Arar Inquiry is *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services, 2006).

40 On some of the challenges, see Martin Rudner, "Towards a Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism" and Wesley Wark, "The Intelligence-Law Enforcement Nexus" in Vol. 1 of Research Studies: Threat Assessment RCMP/CSIS Co-operation.

inquiry is to make information available to the public and to build an accessible and permanent foundation for further research into the area.

The four volumes of research studies published at the same time as the Report are organized thematically. Each contains an introduction which summarizes the content of the papers. The first volume examines the threat of terrorism, threat assessment and RCMP/CSIS cooperation.[41] The second volume deals with terrorism financing and charities.[42] The third volume examines the challenges of terrorism prosecutions, including witness protection.[43] The fourth volume, written by the Commission's Director of Research (Legal Studies), Kent Roach, focuses on the relationship between intelligence and evidence.[44]

2.2 Managing the Proceedings and Inherent Challenges

At the outset of the Commission proceedings, the Commissioner expressed the hope that the Inquiry could proceed effectively and efficiently, noting that the Commission would be judged by its effectiveness and not by its length.[45] As stated in the Arar Report, "…in order to be effective, a public inquiry must also be *expeditious*."[46] The expeditious conduct of an inquiry can contribute to significantly diminishing the cost of the inquiry to the public. Further, it allows the Inquiry to remain relevant and "…makes it more likely that members of the public will be engaged by the process and feel confident that their questions and concerns are being addressed."[47] In the present Commission, while the events inquired into were removed in time, it remained important to attempt to avoid unnecessary interruptions and delays to allow ongoing public engagement in the issues once the public interest in this matter was revived. Furthermore, given the delay between the events and the Inquiry, the families deserved to obtain the long overdue answers they had been seeking as quickly as possible.

---

41 The first volume contains the following papers: Bruce Hoffman, "Study of International Terrorism"; Michael A. Hennessy, "A Brief on International Terrorism"; Peter M. Archambault, "Context is Everything: The Air India Bombing, 9/11 and the Limits of Analogy"; Martin Rudner, "Towards a Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism"; Wesley Wark, "The Intelligence-Law Enforcement Nexus"; and Jean-Paul Brodeur, "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures."

42 The second volume contains the following papers: Nikos Passas, "Understanding Terrorism Financing"; Anita Indira Anand, "An Assessment of the Legal Regime Governing the Financing of Terrorist Activities in Canada"; David G. Duff, "Charities and Terrorist Financing: A Review of Canada's Legal Framework"; Mark Sidel, "Terrorist Financing and the Charitable Sector: Law and Policy in the United Kingdom, the United States and Australia"; and Kathleen Sweet, "Canadian Airport Security Review."

43 The third volume contains the following papers: Yvon Dandurand, "Protecting Witnesses and Collaborators of Justice in Terrorism Cases"; Robert M. Chesney, "Terrorism and Criminal Prosecutions in the United States"; Bruce MacFarlane, "Structural Aspects of Terrorist Mega-Trials: A Comparative Analysis"; and Kent Roach, "The Unique Challenges of Terrorism Prosecutions."

44 Kent Roach, *The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence.* A summary of this study is also contained in the third volume.

45 Opening statement by the Commissioner, Transcripts, June 21, 2006.

46 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006),p. 282
[Emphasis in original] [*Arar Report*].

47 *Walkerton Report,* p. 473.

Regrettably, the Commission's ability to conduct its hearings expeditiously was complicated by the delay of more than 20 years in establishing this Inquiry. In addition to depriving the families for many years of the answers they deserved and of the opportunity to have their stories heard publicly, the time that had transpired since the bombing of Air India Flight 182 introduced a layer of additional complexity to the Commission's process. The fact that the Government had allowed such a significant amount of time to elapse before calling an inquiry was in large part responsible for making the process more difficult, lengthier and more costly than it otherwise needed to have been. A vast amount of documentation accumulated over the years which then had to be reviewed and analyzed in order to find and select relevant documents. The dated files were more difficult to retrieve and search. Some documents, notably those in the possession of the Department of Foreign Affairs and International Trade (DFAIT), have been lost or destroyed. Some individuals involved in crucial events have died. Others have had their memories of events fade or even disappear. In the end, the Commission had to rely to a large extent on a documentary record that was difficult to assemble and understand, without always being able to obtain first-hand evidence from live witnesses.

The documents, when available, often constituted the best and sometimes the only evidence that could be relied on, since they recorded the events as they happened, with no alteration resulting from the passage of time. However, significant time and effort were required to reconstitute a narrative ranging over 20 years, in many cases without the benefit of the memories or explanations of the individuals involved, and on the basis of documents that were not always self-explanatory. To prepare and present comprehensive evidence about all facts and events would have required years of Inquiry hearings. To address this and the added complexities resulting from the Inquiry's broad mandate, which called for the examination of a wide range of complex issues, the Commission had to devise special procedures. Commission dossiers and an episodic approach to the evidence were used to make sense of the factual, historical and other relevant evidence and to relate it to the Terms of Reference. This combination of tools helped sharpen the focus and maximize the efficiency of the Commission's approach to its work.

Commission dossiers contained a concise statement of facts based on other examinations of the circumstances surrounding the Air India bombing,[48] as well as on other reliable public sources.[49] Their main purpose was to provide a factual introduction to the specific subject matter to be dealt with and to set out relatively uncontroversial facts to allow the Inquiry hearings to focus on the heart of the more complex or controversial issues relevant to each topic. The evidence heard by the Commission related to events occurring over many years and could not always be presented chronologically if it was to be related to the substantive issues examined. The dossiers could be used to situate the

---

48 The Commissioner could accept these as conclusive or assign them the weight he deemed appropriate.

49 As set out in Rule 42 of the *Rules of Procedure and Practice*, the dossiers could contain a "…statement of evidence, facts or conclusions together with the sources or basis for the evidence, facts or conclusions that Commission counsel proposes that the Commissioner adopt…".

evidence heard within a broader context and to provide a better appreciation of its relevance.[50] As a result, it was possible to present evidence relating to specific events or issues occurring in different time periods without losing sight of the surrounding circumstances and context. Substantive links between apparently separate and unrelated events could be made and trends and patterns could more easily be identified. Further, the dossiers provided an appreciation of the previous state of public knowledge which could then be compared with the new information learned during the Inquiry – a comparison that demonstrates that the families were justified in their persistence to demand a public Inquiry in spite of the previous reviews and examinations that had been conducted.[51]

While it was explicitly contemplated that statements made in the Commission dossiers could be refuted by the evidence presented before the Inquiry,[52] the use of dossiers nevertheless contributed to making the process more efficient. The dossiers eliminated the need to present evidence about peripheral or uncontroversial issues. As a result, the Commission's time and resources were not wasted on the resolution of unimportant debates and could be more fully devoted to the most important issues, without losing sight of the broader historical context.

The Commission also adopted a concrete, episodic approach to the actual evidence heard, rather than an abstract or purely narrative approach. For example, Phase I of Stage 2, focusing on the law enforcement and intelligence response to Sikh terrorism, began with the examination of a number of episodes or "critical incidents" that allowed the Commission to trace the manner in which specific pieces of information relevant to threat assessment and response were handled prior to the bombing.[53] This provided concrete examples capable of being used as a prism to examine the general structure of the threat assessment process, the general flow of threat information and the adequacy of the measures put in place to respond to the threat. The 1985 regime could thus be examined with a view to identifying specific deficiencies and to understanding the changes, if any, necessary to correct the deficiencies and prevent the recurrence of any identified failures. This episodic approach was used to an even greater extent for the evidence relating to the investigation into the Air India bombing. Given the time period involved and the quantity of material

---

50 See, generally, the explanations provided by Lead Commission Counsel Mark J. Freiman in his Opening statement, Transcripts, vol. 1, September 25, 2006, pp. 5-6 and in his Opening statement, Transcripts, vol. 15, February 19, 2007, p. 1381.

51 In some cases, specifically with respect to factual and historical evidence, the summary of publicly available materials contained in the dossiers was considerably supplemented by the documentary record and evidence heard before the Commission, in light of the limited amount of materials previously available. See, in particular, Exhibit P-102: "Dossier 2: Terrorism, Intelligence and Law Enforcement – Canada's Response to Sikh Terrorism", February 19, 2007.

52 See Opening statement by Mark J. Freiman, Transcripts, vol. 15, February 19, 2007, pp. 1381-1382. With respect to Dossier 2, it was stated that no position was taken by Commission counsel as to the correctness of the various positions adopted and conclusions reached by persons and institutions, as documented in publicly available materials, which were set out in the Dossier.

53 See generally, the explanations provided by Lead Commission Counsel Mark J. Freiman in his Opening statement, Transcripts, vol. 20, April 30, 2007, pp. 1869-1870. Freiman noted that one of the episodes, the Parmar warrant critical incident, also related to the specific process which was used to fill a known information gap.

available, the presentation of a detailed narrative would have been impractical and inefficient. Instead, a number of episodes or incidents that occurred during the course of the investigation were examined in detail during the hearings because they spoke directly to the issues at the heart of the Inquiry's mandate and they illustrated both the serious challenges encountered and the practical consequences which resulted.[54]

The episodic approach to the evidence, in addition to contributing to making the inquiry process as focused and efficient as possible, sought to capture the issues as they presented themselves rather than to look for complete historical evidence. This allowed for the creation of order out of chaos by relating the factual evidence to the substantive issues to be examined. It enabled the Commission to review concrete illustrations in a manner that would not have been possible if a detailed mining of all documents had been undertaken. The critical incidents examined during the Inquiry hearings provided the Commission with an appreciation of how the general theoretical issues and challenges manifested in practice, how they were dealt with and what concrete consequences resulted. This contributed to focusing the Inquiry by ensuring that the examination of any deficiencies and the formulation of any recommendations to address those deficiencies remained grounded in reality, and took into account the real difficulties faced by the members of the security intelligence and law enforcement communities engaged in the prevention and investigation of terrorism.

2.3 Special Procedural Challenges

In addition to the inherent challenges associated with the nature of the Inquiry's mandate and, most importantly, with the passage of a significant amount of time since the events, several specific procedural issues posed additional challenges for the Commission. In some cases, those issues impacted on the substance of the evidence that could be heard and required the use of creative solutions to ensure that all relevant matters would be addressed. In other cases, most notably that of NSC claims, the issues had a significant impact on the Commission's ability to proceed efficiently and expeditiously.

2.3.1 The Importance of Public Hearings

Because of the redaction reconsideration process, which the Government ultimately agreed to engage in, it was possible to hold the Inquiry hearings in public. As a result, a considerable amount of new information could finally be revealed to the public. Contrary to what may have initially appeared to many of those closely involved with this Inquiry,[55] the holding of *in camera* hearings was not necessary in order to discharge the Commission's mandate. The only *in camera* hearing held in the course of the 85 days of Stage 2 hearings was one brief hearing in November 2007, respecting a motion by Government that

---

54 Statement by Mark J. Freiman, Transcripts, vol. 46, September 17, 2007, p. 5515.

55 See, for example, the Opening statement by Barney Brucker, Transcripts, vol. 12, November 6, 2006, p. 1065 and Opening remarks by Barney Brucker, Transcripts, vol. 15, February 19, 2007, p. 1377.

certain matters not be heard in public.[56] Some affidavit evidence was filed by the Government, but no oral evidence was heard. In the end, Commission counsel and Government counsel were asked to pursue discussions that resulted in an agreement on the evidence that could be filed. "Admissions" addressed to the content of a number of specific documents were filed and a lengthy Agreed Statement was entered covering the entire content of the information that could be made public about "Mr. A".[57] A similar process of filing an Agreed Statement or Chronology containing summaries of documents had been used in the spring of 2007 for the "November 1984 Plot Chronology". The general approach adopted by the Commission was to resort to such summaries or admissions only where the production of original documents remained impossible without extensive redactions that would render them meaningless, and where the information included in the summaries was considered sufficient for purposes of advancing the Inquiry within the terms of the mandate.

While it is possible in the context of a Commission of Inquiry to hear and receive some evidence *in camera* and while the Terms of Reference for this Commission specifically provide for this contingency,[58] the fundamental nature of a public inquiry must remain, as the name indicates, public. It is essential that the proceedings of a public inquiry "…be as transparent, accessible and *open to the public* as possible."[59] After all, "…one of the main purposes of an Inquiry is to enable concerned citizens to learn firsthand what occurred …"[60] The "…public desire to learn the truth"[61] will generally be fully satisfied only through a process that is completely transparent and that involves hearings fully accessible to the public. As indicated by Commissioner John Gomery:

> By following the public hearings, [concerned citizens] are able to arrive at informed opinions as to who might be held responsible for any errors or mismanagement that might have occurred affecting what the *Inquiries Act* calls "the good government of Canada". The first role of the Commissioner is to conduct hearings that serve to facilitate the understanding of the public…[62] [Emphasis added]

---

56 See Statement by Mark J. Freiman outlining the issues at stake, Transcripts, vol. 12, November 6, 2007, pp. 8996-8997. An *in camera* hearing was also called on June 20, 2007 but could not proceed as a result of the Commission's inability to offer absolute assurances to the witnesses that their evidence would never become public: Remarks by the Commissioner, Transcripts, vol. 45, June 20, 2007, pp. 5481-5482.

57 See Opening remarks by the Commissioner, Transcripts, vol. 75, November 14, 2007, p. 9371 and Opening remarks by Mark J. Freiman, Transcripts, vol. 75, November 14, 2007, pp. 9373-9375.

58 P.C. 2006-293, para. (m)(i)-(iii).

59 *Arar Report*, p. 282 [Emphasis in original].

60 John H. Gomery, *Fact Finding Report*, Commission of Inquiry into the Sponsorship Program and Advertising Activities, p. 10 [*Gomery Report*].

61 *Phillips v. Nova Scotia (Commission of Inquiry into the Westray Mine Tragedy)*, [1995] 2 S.C.R. 97, para. 175 (Cory J.).

62 *Gomery Report*, p. 10.

Justice Samuel Grange, who presided over the Inquiry into Certain Deaths at the Hospital for Sick Children, discussed the important role of inquiries in informing the public and the value of the presentation of evidence in public, even apart from the other benefits associated with public inquiries. He wrote:

> I remember once thinking egotistically that all the evidence, all the antics, had only one aim: to convince the commissioner who, after all, eventually wrote the report. But I soon discovered my error. They are not just inquiries, they are *public* inquiries… I realized that there was another purpose to the inquiry just as important as one man's solution to the mystery and that was to inform the public. Merely presenting the evidence in public, evidence which had hitherto been given only in private, served that purpose. The public has a special interest, a right to know and a right to form its opinion as it goes along.[63] [Emphasis added]

Allowing the public to learn all the facts which will form the basis of the Commissioner's conclusions and recommendations and to witness the unfolding of the process is therefore crucial. As indicated by Commissioner Dennis O'Connor in the Arar Report:

> Openness and transparency are hallmarks of legal proceedings in our system of justice. Exposure to public scrutiny is unquestionably the most effective tool in achieving accountability for those whose actions are being examined and in building public confidence in the process and resulting decision.[64] [Emphasis added]

These fundamental principles should only be derogated from in truly exceptional cases, where real harm could be done to legitimate interests through the disclosure of information. The information sought to be kept secret should be as limited as is possible, and the premise should always be that hearings are to be held in public unless it is absolutely impossible.

In this Inquiry, the public nature of the hearings was particularly important in light of the fact that the families, those most affected by the events that made the Inquiry necessary, had been promised a full public inquiry. The Terms of Reference for the Commission recognize the importance of granting the families of the victims an "…opportunity for appropriate participation" in the Inquiry.[65] Under the circumstances, and in light of the burden the families bore as a result of the bombing and of the efforts they made for over 20 years to ensure that

---

63 S.G.M. Grange, "How should lawyers and the legal profession adapt?" in A. Paul Pross, Innis Christie and John A. Yogis, eds., *Commissions of Inquiry,* Dalhousie Law Journal, vol. 12 (1990), 151, pp. 154-155.

64 *Arar Report*, p. 304.

65 P.C. 2006-293, para. (f).

a public inquiry would take place, "appropriate participation" required nothing less than receiving a full opportunity to hear and see the evidence. Had this evidence been heard *in camera*, the families and their counsel would have been excluded.[66] Any summaries of the *in camera* evidence issued by the Commission would have been subject to vetting by the Government, which could have again asserted National Security Confidentiality (NSC) claims that would have prevented portions of the information from being made available to the families and to the public. Counsel for the families would have been unable to cross-examine Government witnesses testifying about crucial issues. Given that most of the information the Government sought to redact was 15 to 20 years old and related to historical events with little connection to the present security context, this type of proceeding was not necessary, and would neither have led to meaningful participation by the families nor to the "appropriate participation" contemplated by the Terms of Reference.

Further, the Commission was mandated to inquire into and make recommendations about broad policy issues of interest to the public at large. The methods available to the law enforcement and security intelligence communities to combat terrorism and protect human life, as well as the limits placed on those methods as a result of policy decisions or deficiencies in the existing regime, are of interest to all members of the public. Under the circumstances, it was of the utmost importance that not only the families of the Air India victims, but all members of the public be provided with an opportunity to follow the proceedings of the Commission so that they might learn first hand about the evidence presented, and be able to assess the issues and form their own opinion about the facts, the deficiencies identified, if any, and the eventual recommendations meant to improve Canada's ability to prevent and prosecute acts of terrorism.

2.3.2 The Impact of NSC Claims

While in the end it was possible to achieve the goal of holding full public hearings, the NSC issues which had to be addressed throughout the proceedings nevertheless did have a serious impact on the process of this Inquiry. A great deal of time and considerable resources were expended dealing with NSC issues. These issues caused delay in the progress of the hearings, and were the major force behind a delay in the Commission's proceedings for most of the period between November 2006 and the end of April 2007. The NSC claims reconsideration process, which continued throughout the remaining months of Commission hearings, in some cases caused further delays and required adjustments in the hearings schedule to await documents becoming available with fewer redactions and in all cases consumed significant resources both

66 See *Reasons for Decision with Respect to the AIVFA's Request for Directions Regarding Access to Unredacted Documents and In Camera and Ex Parte Hearings* in Annex A of this Volume, which concluded that the Terms of Reference precluded the Commissioner from granting AIVFA counsel access to any *in camera* hearings and unredacted documents, and that, in any event, even if such access had been possible, counsel would have been precluded by law from sharing the information acquired with the families.

for the Commission and the Government legal teams. Those resources had to be diverted to reviewing NSC claims, even though many requests for new documents and information remained pending and much remained to be done to work through and prepare the substance of the evidence to be presented before the Commission.

Further, the final versions of documents often could not be made available to counsel for the Parties as far in advance of the hearings as would have been desirable. This was especially troubling with respect to the victims' families, given the express mandate in the Terms of Reference calling for their "meaningful participation."[67] Because of the time necessary to complete the redaction reconsideration process, the families frequently received the final redacted versions of the documents a few days before the hearings and sometimes only a few hours before. This required counsel for the families to attempt instantly to absorb an important amount of entirely new information. The challenge this represented must be recognized. Since most of the witnesses were present or former Government agents or employees and therefore would have been privy from the start to all of the information initially subject to redaction (as were counsel for the Government), the witnesses and Government counsel had much more opportunity to prepare in advance than did counsel for the families. To make matters worse, because the will say statements containing a description of the witnesses' anticipated evidence and lists of associated documents also had to be vetted for NSC purposes, counsel for the Parties also often did not have the benefit of this information as far in advance of the hearings as would have been desirable. The dedication of counsel for the Parties was of great assistance in overcoming these challenges wherever possible, and in ensuring the meaningful participation of the families in this Inquiry.

Under the circumstances, Commission counsel were called upon to conduct more searching examinations than would otherwise have been necessary to ensure that all relevant issues were explored. While this was, in some respects, different from the role normally assumed by Commission counsel in public inquiries, it was necessary in order to compensate for the challenges associated with the late disclosure of large volumes of documents and information. As indicated by Commissioner O'Connor in the Arar Report, the fact that Commission counsel may, in such circumstances, have to depart from their usual role need not result in their adopting an adversarial role or taking a prosecutorial stance, both of which would be contrary to their duty to lead evidence in an independent and fair manner.[68] In this Inquiry, the occasionally somewhat more active role of Commission counsel was, to the contrary, necessary to ensure that the evidence was presented fairly and completely. In this respect, the role of Commission counsel could best be described as "inquisitorial" rather than "adversarial" and reflects the status of the Commission as an Inquiry.

---

67 P.C. 2006-293, para. (f).

68 *Arar Report*, pp. 292-293. In the Arar Commission, the circumstances required the actual cross-examination of witnesses by Commission counsel in the absence of counsel present to represent the interests of other parties.

2.3.3 The Nature of the Government's NSC Claims

Because of their impact on the process of this Inquiry, and because of the challenges they posed for non-government Parties, the nature and extent of the Government's initial NSC claims deserve comment. The extent of the Government's reconsideration of its own claims is helpful in understanding whether the unfortunate consequences of the original NSC claims on the process of the Inquiry could have been avoided. Essentially, a large number of documents that were entirely blacked out in the version initially provided to the Parties ended up being produced with few if any redactions.[69] In the Arar Report, Commissioner O'Connor described a phenomenon he referred to as "overclaiming", which involved the Government maintaining NSC claims over a great deal of information throughout the proceedings of the Commission and then conceding after the fact that the information in question could in fact be publicly disclosed.[70] Commissioner O'Connor explained that the Government engaged in a review of redactions and modified its position with respect to many of its initial NSC claims near the end of the public hearings, or after the hearings were completed. As a result, in the Arar Inquiry some of the information over which the Government initially claimed NSC was eventually disclosed without challenge, but not always in time for the evidence to be heard in public. Unfortunately, the term "overclaiming" also aptly describes the Government approach to NSC claims in the present Inquiry.

The differences between the various versions of redacted documents provided by the Government over the course of the Inquiry leave little doubt about the extent of the unnecessary NSC claims that were initially made. After reconsideration, the Government itself concluded that much of the redacted information could in fact be publicly disclosed without compromising national security.

The February 2007 redactions rendered many key documents meaningless and thus made the conduct of public hearings impossible at the time.[71] Yet, after the Government reconsidered its original redactions, it became possible to conduct all of the Commission's hearings in public, using the very documents that had originally been redacted beyond any potential use. This "overclaiming" continued throughout the Inquiry process. Redaction reconsideration requests continued to be necessary not only for the very first set of redacted documents provided by the Government prior to February 2007, but also for new documents redacted by the Government over the summer and into the fall of 2007 and beyond. Many of the documents provided after the conclusion of the hearings continued to be subject to wide initial NSC claims.

---

69 See, for example, Exhibit P-101 CAC0403, re-entered as CAC0403(i) on May 3, 2007 and Exhibit P-101 CAB0073, re-entered as CAB0073(i) on June 18, 2007. The majority of the most striking examples are not referred to here as the very first versions produced by the Government were not entered into evidence in light of their lack of usefulness as a result of the extensive redactions.

70 See, generally, *Arar Report*, pp. 301-303.

71 See Opening statement by the Commissioner, Transcripts, vol. 15, February 19, 2007, pp. 1370-1371.

Since the reconsideration process continued after redacted versions of the documents were entered into evidence,[72] it is now possible to appreciate, at least to some extent, the nature and extent of the overclaiming of NSC by the Government. A few examples of the evolution of the redactions are instructive in this respect.

The Commission heard evidence about CSIS contacts with a person referred to as Ms. E, who eventually testified in the criminal trial of Ajaib Singh Bagri and Ripudaman Singh Malik. The CSIS agent who dealt with Ms. E, William Dean ("Willie") Laurie, had prepared reports about his conversations with Ms. E, where his position and that of his superiors on the issue of whether and when her information should be passed to the RCMP was discussed. Despite the fact that those issues went to the heart of the Commission's mandate and that Laurie had testified extensively in public proceedings before the Supreme Court of British Columbia in the Malik and Bagri trial about the content of the reports,[73] all comments respecting the passing of the information to the RCMP were redacted in full in the versions initially produced by the Government.[74] New versions of the documents had to be entered in evidence on October 15, 2007, after the Government reconsidered and eventually abandoned its NSC claims.[75]

The Commission also heard evidence about the security measures put in place by the RCMP at Pearson and Mirabel airports prior to the Air India bombing. One document contained a grid of the security measures corresponding to various security levels used in 1985. This document was initially produced to the Parties with its contents fully blacked out. These redactions were reconsidered by the Government and, in the end, the document was filed with no redactions at all.[76] Nevertheless, information from this document continues to be blacked out in full in another, identical document in the evidentiary collection.[77]

The Commission requested documents from Air India and Air Canada in connection with the aviation security evidence. Having reviewed the documents, Commission counsel provided copies to counsel for the Government. The Government took the position that information found in those documents, though not provided by the Government to the Commission, had to be redacted pursuant to the *Aeronautics Act*.[78] The Commission agreed to some of the proposed redactions out of an abundance of caution, but was again forced to request reconsideration of portions of the redactions made by the Government, including redaction of information about the 24-hour hold on cargo imposed by Transport Canada following the Air India bombing, which was clearly already

---

72 Some of the documents contained in the Evidence Binders entered as Exhibit P-101 on May 1, 2007 had already been subject to the redaction reconsideration process, while others had not.
73 See Trial Transcripts: Exhibit P-244.
74 See Exhibit P-101 CAA0553, CAA0562, CAA0579.
75 Exhibit P-101 CAA0553(i), CAA0562(i), CAA0579(i).
76 See Exhibit P-101 CAA0025.
77 See Exhibit P-101 CAA0027.
78 R.S.C. 1985, c. A-2.

public. The Government finally agreed to lift some of its more egregious claims on the day before the documents were to be entered into evidence[79].

The Commission heard evidence from members of the Integrated Threat Assessment Center (ITAC), who testified about the threat assessments prepared by ITAC. In this context, it was learned that ITAC, where possible, produces unclassified versions of its threat assessments intended for broader circulation. However, the illustrative unclassified threat assessment which was initially provided to the Commission surprisingly emerged from the review process heavily redacted.[80] Another version, completely unredacted this time, was finally entered into evidence after the Government again reconsidered its position.[81]

In addition to these examples, it should be noted that counsel for the Government stated before the Commission on March 5, 2007 that, in response to the Commissioner's February 19th call for more information to be made available to the public, Government agencies not only began reviewing their own NSC claims, but also contacted the Vancouver Police Department and the Government of India to obtain permission to release information provided under caveats.[82] This permission was obtained in many cases, and a large number of the documents that were initially redacted in full were released in the public hearings.[83] The process would have been expedited for all involved if this authorization had been sought and obtained right from the start rather than having the documents initially provided in redacted form.

This apparently reflexive application of third party caveats, without requesting that the caveats be lifted, finds echoes in continuing CSIS practices that are discussed in Volume Three and that have been the subject of critical comment from the judiciary, notably in the *Khawaja* case.[84] In fact, the Attorney General of Canada argued in its Final Submissions to this Inquiry that"…constant requests to lift caveats would demonstrate that CSIS failed to appreciate their importance."[85] This proposition defies logic, as it would rather seem that requests to lift caveats demonstrate Canada's commitment to respecting caveats and to not using third party information without authorization. The fact that the Government, and CSIS in particular, continues to take this position means that in some cases, as was initially the case in this Inquiry, NSC claims are made with respect to third party information without even asking originators for permission to lift the caveat. In this Inquiry, the failure to take this most basic step contributed to

---

79 Because the documents were not initially provided by the Government to the Commission, the Government further requested that the Commission physically redact the documents itself, causing further delay for the Parties who were waiting to receive disclosure of the materials.

80 Exhibit P-101 CAF0542.

81 Exhibit P-349.

82 Statement by Barney Brucker, Transcripts, vol. 16, March 5, 2007, pp. 1415-1416.

83 See, for example, the "June 1st Telex," authorized for release by the Government of India (Exhibit P-101 CAA0185) and the "Khurana report," authorized for release by the Vancouver Police Department (Exhibit P-101 CAC0487), which were both crucial documents in these proceedings that were initially redacted in full and later released with practically no redactions.

84 *Canada v. Khawaja*, 2007 FC 490, para 146.

85 Final Submissions of the Attorney General of Canada, Vol. I, para. 487.

slowing down and complicating the process unnecessarily, as well as making it more difficult for other Parties.

The Government's efforts to reconsider its initial NSC claims must be commended.[86] An impressive amount of time and effort was expended by Government officials in the redaction reconsideration process in order to make documents available to the public. Nevertheless, the extent of the reconsideration engaged in also shows that the negative impact on the Inquiry could have been avoided to a large extent if the Government had appropriately limited its initial NSC claims to what was truly necessary. While the consequences of Government overclaiming on the process of the present Inquiry were not as severe as in the Arar Commission (where Commissioner O'Connor indicated that NSC issues not only lengthened the process by approximately 50 per cent,[87] but prevented the Commission from actually hearing in public evidence which could have and should have been heard publicly[88]), the waste of public resources for the present Inquiry was not negligible.

Prior to the Arar Commission, there was no precedent for redacting documents for NSC concerns in the context of a public inquiry.[89] Commissioner O'Connor formulated his comments about NSC overclaiming in the hope that his experience could provide guidance in other cases. He indicated that:

> In legal and administrative proceedings, where the Government makes NSC claims over some information, the single most important factor in trying to ensure public accountability and fairness is for the Government to limit, from the outset, the breadth of those claims to what is truly necessary.[90] [Emphasis added]

Unfortunately, Commissioner O'Connor's efforts in raising the issue for the future had little impact on the Government's approach to NSC claims in this Inquiry. It must be reiterated in the strongest terms that Government NSC claims should never be "an opening bargaining position."[91] There is no room for negotiation strategies in the realm of national security confidentiality, both because the legitimate interests that actually require protection are of the utmost importance and because the principles of public accountability and fairness require that such claims be limited from the outset to what is truly necessary to protect vital interests.

---

86 See *Arar Report*, p. 303, where Commissioner O'Connor also recognized this.
87 *Arar Report*, pp. 279-280.
88 *Arar Report*, pp. 301-302.
89 *Arar Report*, p. 302.
90 *Arar Report*, p. 304.
91 *Arar Report*, p. 302.

A significant consequence of NSC overclaiming is that it "…promotes public suspicion and cynicism about legitimate claims by the Government of national security confidentiality."[92] In many cases, there will be a legitimate Government interest in protecting the identity of informants, in preserving the integrity of ongoing national security investigations and in preserving the confidence of foreign governments who provide information vital to the protection of Canada's national security.[93] When seeking to protect such important interests, it may be understandable that some Government officials may choose "…to err on the side of caution in making NSC claims."[94] However, NSC overclaiming ultimately harms the very interests that national security confidentiality is meant to protect. The less seriously NSC claims are taken, the more breaches are likely to occur.

Further, overclaiming also promotes public suspicion and cynicism toward Government institutions in general. If a significant volume of NSC claims are shown to have been made unnecessarily, there is a risk that members of the public will conclude that the Government is attempting to hide embarrassing information, as opposed to protecting legitimate national interests, thereby undermining public confidence in our national security establishment. In his testimony before the Inquiry, former RCMP Commissioner Giuliano Zaccardelli commented on the tendency to overclassify information which he observed in federal agencies and on its impact on Government:

> **MR. FREIMAN:** […] There's been some reference in our hearings to a culture of secrecy that pervades Ottawa. Do you have any comment on that characterization?
>
> **MR. ZACCARDELLI:** I think it's an accurate characterization.
>
> **MR. FREIMAN:** Accurate or inaccurate?
>
> **MR. ZACCARDELLI:** Accurate. It's accurate. We over classify, we over-redact and then we ultimately get embarrassed by it being shown to not have been necessary so many times. I think it's just in the nature of the beast, and that happens all the time, and it happens continuously before every inquiry that seems to take place. We start from the position of we're not going to share, we're not going to show anything because we don't want to reveal anything and then, ultimately, we have to reveal, and we have to show, and the system gets embarrassed because of some obvious, you know, classifications that were clearly inappropriate and so on.

---

92 *Arar Report*, p. 302.
93 See, generally, Opening statement by Barney Brucker, Transcripts, vol. 12, November 6, 2006, p. 1064.
94 *Arar Report*, p. 302.

> And I don't think there's any malice intended by anybody at all when they do this. They honestly believe this is what we have to do. But it's shown in the end that it doesn't work...[95]

The evidence heard before the Inquiry demonstrated that the culture of secrecy, the extensive use of caveats, the exaggerated reliance on the "need-to-know" principle and the over-claiming of national security confidentiality that occurred throughout the pre-bombing threat assessment process and through the Air India investigation itself have been a source of significant conflict among the agencies and a significant hindrance to the criminal prosecutions. This culture of secrecy may well have deprived important actors of crucial information that might have assisted in preventing or solving the Air India bombing. One of the fundamental questions posed by the Terms of Reference for this Inquiry is whether the Government agencies involved in the lead-up to and the aftermath of the bombing have learned the necessary lessons from their past mistakes. The continued overclaiming of NSC observed in the initial stages of this Inquiry, occurring as it did immediately after this very problem was identified in the Arar Inquiry and after the results of the problem could clearly be observed in the Air India case itself, is not encouraging. Nor is it encouraging that aggressive NSC claims continued throughout the hearings in this Inquiry, and even after the conclusion of the hearings. As well, it is not encouraging that Government had not initially requested the lifting of caveats by the originator before claiming NSC over a large portion of materials which could be released in the end, nor that Government nevertheless continues to take the position that requests to lift caveats need not always be made before NSC is claimed.

It must also be noted that, even with the reconsideration process, a number of the redactions that remain appear unnecessary for purposes of protecting national security though, to be sure, the endless hours spent negotiating the lifting of redactions of words and paragraphs, and turning specific references into more generalized ones, did result in most, if not all, of the key information being made available in some form to the public.

It can only be hoped that the Air India bombing and the experience of this Inquiry will encourage the Government to further refine its process for NSC claims to ensure that such claims are more effectively tailored and limited to what is truly necessary to protect Canada's national security.

2.3.4 Identification of Relevant Information

The collection of documents in preparation for the Inquiry posed serious challenges both for the Government and the Commission. In light of the variety and complexity of the subject matters to be inquired into, the number of government agencies and departments involved and the length of time elapsed since the events, it was extremely difficult to discover and isolate the

95 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11082.

documents relevant to the Inquiry's mandate. The document collection and redaction process was further complicated by the extensive negotiations with the Government relating to identification of relevant documents and information and by the resulting delays in obtaining the necessary materials.

In fairness to the Government officials involved, they faced an extremely challenging task. Many thousands of documents could potentially fall within the ambit of the Terms of Reference,[96] and a large number of those had to be reviewed for relevancy and thereafter for NSC. Under the circumstances, it is not surprising that the Government sought to obtain as much clarification as possible respecting the Commission's interests to assist in narrowing the search parameters to select the most appropriate documents. Government officials were willing to work with the Commission to find creative solutions to overcome the challenges arising from document selection and redaction processes. Helpful discussions with Commission counsel achieved a clearer identification of the most important documents. In some cases, access to government offices was provided and the Commission staff were allowed to review the available documents or databases in order to formulate more specific requests. Knowledgeable staff from the various government agencies was made available to assist the Commission in its review of government files.

However, frequent lengthy meetings and correspondence with counsel for the Attorney General of Canada (AGC) imposed large time and resource requirements, as the Government sought to obtain an increasing level of detail about the scope of Commission counsel's requests for documentary disclosure and about the precise redacted information sought to be reconsidered. Too often, those discussions became an occasion for the Government to argue its views about the relevance to the Inquiry's mandate of the information being requested or being sought to be made public. For example, when information was first requested about what would become known as "the Mr. A. story", which illustrated many of the issues at the heart of the Inquiry's mandate, Government counsel advised in December 2006 that this avenue of inquiry led nowhere and would only result in "…a tremendous waste of time and resources at the expense of matters germane to the Terms of Reference." In another case, a redaction request for extracts of a report respecting protective policing issues in the period immediately preceding the bombing was challenged as not being relevant to the Inquiry.

Such discussions were also common in the context of the NSC vetting process for will say statements, where Government counsel provided comments that addressed not only NSC issues, but also the actual content of the anticipated evidence, including arguments about the relevance, appropriate interpretation or fairness of the evidence which Commission counsel proposed to lead.[97] In some instances, Government counsel requested changes to the will say

96 See Statement by Barney Brucker, vol. 19, March 9, 2007, p. 1769.

97 Those types of comments were received on a regular basis during the "will says" vetting process, while actual NSC issues were seldom raised in that context.

statements that were contrary to what the witnesses had said in interviews, but fit better with Government counsel's view of what the witnesses meant or with their suggested interpretation of what was said.[98]

In addition, an unduly narrow view, not appropriate in the context of a public inquiry, was at times adopted by the Government in its interpretation of Commission requests and of the Government's obligations. In some cases, attempts were made to provide only as much of a response as was absolutely required, taking the narrowest view of the request. Equally disconcerting, Commission counsel were not always advised promptly when documents of interest were located by the Government prior to being specifically requested by the Commission. At times this tardiness simply constituted a minor annoyance. Thus, when discussions began between Government counsel and Commission counsel to create what would become the "November 1984 Plot Chronology", Government counsel used its own set of materials, not previously disclosed to the Commission, to prepare a proposed Agreed Statement and only provided those additional materials to the Commission some weeks later. On other occasions, the consequences were more serious and threatened unfairness to witnesses. Notably, during the cross-examination of Brian Simpson, Government counsel sought to rely on documents that had been identified from the civil litigation file, without providing prior notice of the specific documents upon which they would be relying.[99] Not only was Simpson cross-examined with a view to impugning his credibility on the basis of a description of documents that no one outside of Government and its counsel had previously seen, but the full documentary record turned out, in fact, to include a document that corroborated aspects of his testimony that were being challenged.[100] The Government has tried to explain away its reliance on these previously unseen documents, in part, on the basis that they were included in an RCMP database compiled for purposes of the Air India criminal trial that was made available to Commission counsel in the summer of 2006.[101] This collection consisted of tens of thousands of unindexed documents housed in a document management system that was different from the one the Department of Justice insisted be used by the Commission and that was capable of being searched in only the most rudimentary manner. The Commission does not accept that in effect inviting Commission counsel to sift through this unwieldy mountain of data constituted adequate production of relevant documents let alone effective notice of documents intended to be used to cross examine Simpson.

---

98 This situation continued even after concern was expressed by Commission counsel to counsel for the Attorney General, in correspondence dated June 1, 2007.

99 See Remarks by Mark J. Freiman and Loretta Colton, Transcripts, vol. 32, May 23, 2007, pp. 3714-3715; Remarks by Tracey McCann and Anil Kapoor, Transcripts, vol. 33, May 24, 2007, pp. 3865-3869; and Volume Two: Part 1, Pre-Bombing, Section 1.9, Mr. Simpson's Visit to the Air India Aircraft. It should be noted that the civil litigation file contains over a hundred boxes and was only accessible to Commission counsel upon attendance at government premises.

100 See Volume Two: Part 1, Pre-Bombing, Section 1.9, Mr. Simpson's Visit to the Air India Aircraft.

101 Letter from Government counsel dated May 25, 2007.

Even after Commission counsel asked that all documents identified as relevant by Government counsel be provided immediately to the Commission,[102] and the Attorney General of Canada signaled its recognition that all relevant documents in the Government's possession should be disclosed,[103] there were still instances where the Commission received production of documents, or notice of their existence, weeks, and sometimes months, after its interest in presenting evidence respecting their subject matter was known to the Government.[104] In one particularly egregious case, full disclosure did not occur until many months after the close of hearings.[105]

In the end, the Government's attempts to tailor and narrow the Commission's requests further delayed the proceedings and put the Commission in a position where it was obliged to keep going back with additional requests in circumstances where it could not have had knowledge of the complete documentary record in the Government's possession. By slowing down the entire document collection and redaction process, such situations also contributed to increasing the challenges faced by counsel for the Parties who often received the redacted materials at the last minute. Given the requirement for openness, transparency and fairness in the Inquiry process, full documentary production should not be the subject of a game of "Twenty Questions."

The document collection and redaction process is not the appropriate forum to engage in discussions respecting the nature and extent of what information is or is not relevant, in the Government's view, to the Inquiry's mandate. Nor is the process of vetting of will-says to identify National Security Confidentiality (NSC) issues the appropriate forum to discuss the fairness of inferences taken from the evidence or the accuracy of a witness's evidence. Commission counsel are responsible for representing the public interest and for determining the relevant materials and evidence to be put before the inquiry in public hearings. It is crucial that an inquiry be and appear to be independent from the Government into whose actions it must inquire. As stated in the Arar Report, in order to fulfill "…this duty of independence and impartiality, an inquiry must be *thorough* and examine all relevant issues with care and exactitude, to leave no doubt that all questions raised by its mandate were answered and explored."[106] As a practical matter, this requires that the Commission be provided an opportunity to request and review Government documents and information independently in order

---

102 Letter from Commission counsel to Government counsel dated May 24, 2007.

103 Letter from Government counsel dated May 25, 2007.

104 Examples include the receipt of documents respecting Tara Singh Hayer in late January 2008, when the Commission's interest in presenting evidence about the agencies' dealings with Mr. Hayer was known to the Government since the summer of 2007 and the last witness who testified on this issue was heard in early December 2007, as well as notification in February 2008 of the existence of a VPD report which could clarify aspects of the evidence of Detective Don McLean, who testified in the spring of 2007, and which was apparently located by the RCMP sometime prior to February 11, 2008, but was only provided to Commission counsel after the RCMP went directly to McLean with the report.

105 See Volume Two: Part 2, Post-Bombing, Section 5.7, The present Commission of Inquiry, under the subheading "Stonewalling", as well as the discussion in Section 2.3.7 of the RCMP's failure to disclose information about Mr. G.

106 *Arar Report*, p. 282 [Emphasis in original].

to make its own determinations about their relevance in a manner that does not delay or hinder the preliminary document collection and redaction process. Disputes and disagreements about Commission counsel's selection should take place in the public hearings, where all parties have an opportunity to present their positions subject to public scrutiny.

Similarly, the process used by the Government to present facts and provide information for the consideration of the Commission and of other Parties must be open and transparent. One incident raised concerns in this respect after the close of the hearings. The Attorney General of Canada's Final Submissions contained a substantial amount of new information regarding civil aviation security that had not been canvassed during the Commission's public hearings. As a result, the Commission requested briefings from Transport Canada, with a view to determining whether some or all of the new information should be reflected in the Commission's report.

In all, three briefings were held with Transport Canada officials to address the new information. These briefings related to current aviation security initiatives generally, and to air cargo security and risk management in particular. Commission counsel subsequently prepared summaries of these briefings with the ultimate objective of disclosing their content to the Parties for comment. Because the briefings had entailed discussion of classified and security sensitive information,[107] the briefing summaries were first provided to the Attorney General of Canada (acting on behalf of Transport Canada and other agencies) for redaction and fact-checking.

The manner in which the Government performed the redaction and fact-checking tasks was unsatisfactory.

When the Attorney General of Canada produced the redacted briefing summaries to the Commission, no mention was made of any factual errors identified in the documents. On its face, each document appeared to be a redacted version of the original: that is, a version identical to the original where any passages subject to NSC claims or claims based on the confidentiality that attaches to aviation security measures were simply blacked out. On this basis, the redacted, but otherwise apparently unaltered briefing summaries were disclosed to the Parties shortly after their receipt by the Commission. The Parties were entitled to assume, as had the Commission, that the final text was the result of agreement between the Commission and the Attorney General of Canada as to the substance of the briefings. But this was not the case.

Without any notice or comment, the Government had undertaken to edit the documents for content. Commission counsel did not notice this fact until after production to the Parties, because of the manner in which the changes were made.

---

107 The security-sensitive information discussed at the briefings included aviation security measures made or authorized under sections 4.72 and 4.73 of the *Aeronautics Act*, R.S.C. 1985, c. A-2. Section 4.79 of the Act prohibits unauthorized disclosure of such measures.

It was only in the course of referring to one of the redacted documents that it was noticed that the text on one of its pages appeared oddly positioned. Commission counsel then undertook a detailed line-by-line comparison of the original text and the redacted versions. It was discovered at that point that all three briefing summaries had been substantially altered without the Commission's knowledge or approval. Extensive changes had been made to the original text, in some cases altering the meaning. In one instance, the text was changed so that it not only became an inaccurate reflection of what had been discussed at the briefing, but also constituted an inaccurate statement about a boarding denial under the Passenger Protect Program.[108] Entire portions of text had been added, deleted or modified without any markings to indicate that the documents had been so altered. Indeed, it appears that the Government went to considerable trouble to make the modified summaries look like the originals. Each of the documents had been retyped, using the same format and the same distinctive font as had been used by Commission counsel in the originals.

At one point prior to production, the Attorney General of Canada had made general mention of corrections to one of the documents due to alleged factual errors.[109] No specific details were offered. When the document was later produced as a final product, without any further mention of changes to the text or of concerns with its factual content, this created the false impression that the only changes to the document were the redactions themselves. It was not until the Commission conducted its own detailed analysis and subsequently raised the issue of the unidentified changes, that the AGC then itemized the specific alterations.

The Attorney General of Canada offered a number of reasons why changes to the text were deemed necessary, including disagreements as to factual accuracy, changes to the classification of material discussed at the briefings, changes to the status of aviation security initiatives and even stylistic preferences. However, this cannot explain or justify the lack of notification of the proposed changes. The AGC was free to point out any substantive disagreements it might have had with the contents of the briefing summaries, as it had been invited to do, but the Government was under an onus to clearly articulate the ways in which it wished to alter the documents. As the Attorney General of Canada conceded in subsequent correspondence with the Commission: "…it would have been preferable if delivery of the versions of the briefing summaries had highlighted

---

108 At a briefing on May 14, 2008, Commission counsel requested an update on denials of boarding privileges under the Passenger Protect Program. Transport Canada officials replied that there had been no denials of boarding privileges as of that date. An "action box" indicated that Transport Canada had undertaken to inform Commission counsel should any boarding denial take place in the coming months. This information was reflected at page 11 of the briefing summary prepared by the Commission and submitted to the Government for redaction and fact-checking. In the version of the briefing summary that the Government authorized for release to the parties, the relevant portion of the text was changed to indicate that there had been one boarding denial. In fact, a denial of boarding privileges had not occurred until June 2008 – weeks after the briefing took place. The "action box" was completely removed from the text.

109 The document in question was the May 14, 2008 briefing summary.

or otherwise identified changes or deletions made or that correspondence accompanying delivery had indicated that such changes had been made."[110]

The Commission is prepared to accept the Attorney General of Canada's subsequent assurances that there was no intention to mislead or to frustrate the Commission, but it remains troubling that anyone would have thought it open to the Government to attempt to rewrite Commission documents, let alone that such "corrections" would be undertaken without any mention of the alterations.

2.3.5 Resource Issues

Responding to this Inquiry required a significant investment of time and resources for the Government.[111] Documents had to be constantly reviewed for purposes of redaction and reconsideration of NSC claims, which required input from numerous agencies. Meanwhile, new and pending requests for additional information and documents had to be addressed, and this required Government agencies to identify relevant materials among large collections of documents covering activities ranging over 22 years, some of which were not easily retrievable.[112] Requests relevant to other more policy-oriented Terms of Reference, such as terrorist financing, also had to be processed. In addition, witness interviews had to be arranged and attended, and draft will say statements had to be reviewed for NSC purposes.

In spite of the industrious effort of the Government officials involved, the resources at their disposal were apparently insufficient to enable them to meet the Commission's requests in a timely fashion. Documents were often disclosed or redacted late. Examples include a delay of approximately nine weeks between November 2006 and late January 2007 to obtain a response to a request for information and documents from CSIS, and a delay of almost three full months to obtain a first response to a redaction request for documents relating to the Mr. A story, following which extensive negotiations were necessary to produce an Agreed Statement in lieu of the documents.

In addition to the challenges caused by the delay in calling the public inquiry, which resulted in the accumulation of an unmanageable volume of documents and information, the Commission faced serious obstacles to proceeding efficiently and expeditiously, and counsel for the Parties, in particular the victims' families, had to face additional challenges associated with late disclosure resulting from the lack of sufficient resources available to the Government officials in charge of responding to the Inquiry. This resource insufficiency also contributed to increasing the cost of the present Inquiry to the public by making the overall process lengthier and more complex and plaguing it with protracted and unnecessary discussions about the relevance or appropriateness of the

110 Letter from Government counsel to Commission counsel dated February 13, 2009.
111 For an outline of the various tasks which had to be performed, see Statement by Barney Brucker, Transcripts, vol. 19, March 9, 2007, pp. 1768-1769.
112 Statement by Barney Brucker, Transcripts, vol. 19, March 9, 2007, p. 1768.

Commission's requests, discussions which were in some cases openly driven by the fact that it was simply not possible to mobilize sufficient resources to respond to some of the requests formulated by Commission counsel.[113]

Further, not all Commission requests were processed by the Government prior to the end of the hearings, or in some cases, for months thereafter. As of mid-January 2008, numerous Commission disclosure and redaction requests still remained unanswered, including requests dated July 2007 and October 2007. Not until late March 2008 did those requests finally receive a response. The Commission continued to issue requests in light of its ongoing review of new and existing documents, and responses continued to be provided in a less than timely manner. The last installment of redacted documents was received by the Commission on February 18, 2009, in response to requests made in September and October 2008. It was not until March 2009 that the Government provided a response to another request, outstanding since October 2007, after considerable resources were expended in unnecessary debates over production.

In October 2007, the Commission had requested that a 1985 Transport Canada security audit of Vancouver, Pearson, and Mirabel international airports, conducted immediately after the bombings, be made public. The Attorney General of Canada responded that, because of the limited resources available for the redaction process, consideration of the Commission's request would have to be delayed until November or December 2007. By January 2008, the document had still not been produced and no response had been received from the AGC. Commission counsel followed up on the request, only to be told that Transport Canada now took the position that the document would not be released on the basis of a claim of solicitor-client privilege. It was Commission counsel's view that the audit revealed important details of the inadequate security at some of Canada's largest airports in the spring of 1985, and hence that the production of its contents was important for the Commission's mandate. Although Commission counsel saw no basis for the claim of privilege, in an attempt to reach a compromise, a proposal was made to the Attorney General of Canada in March 2008 that a summary of the document be entered as an agreed statement of fact.

Commission counsel followed up to enquire about the proposal, but no response was received from the Attorney General of Canada until October 31, 2008. At that point, the AGC proposed that the Government would draft its own summary, to be provided within one week. By January 2009, the Government had still not provided any draft summary. Commission counsel again followed up on its request for the public disclosure of either the document itself or a

---

113 Government counsel took issue with some of the Commission's requests because of the amount of material which would have to be reviewed. For example, the Government indicated in July 2007 that one request could not be responded to because the RCMP did not catalogue documents according to subject matter and a review of the entire database would be necessary to respond to the request, which could not be accomplished prior to the completion of the hearings. In another case, the large number of CSIS files involved was invoked to refuse to respond to a Commission request, and the Government subsequently indicated that the Commission's attempts to narrow the request were still not helpful practically in assisting to narrow the scope of the search that would have to be done.

mutually acceptable summary. The AGC's response came in February 2009, at which time it indicated that Transport Canada's position had again shifted. Transport Canada was now reluctant to release any summary of the document, as it was now unwilling to waive any portion of the claim of alleged privilege regarding the contents. Following fruitless discussions about the merits of the privilege claim, Commission counsel made one final attempt at compromise by submitting a list of specific extracts from the report that would be disclosed to the public. Transport Canada officials reviewed the extracts and, in March 2009, the Attorney General of Canada conveyed Transport Canada's refusal to authorize the release of any information. Commission counsel responded by informing the Attorney General of Canada that the audit report would be produced to the Parties by way of disclosure forthwith, and that the Government would have to formally assert any objections it intended to raise on the basis of alleged privilege through available legal means.

Immediately thereafter, the Attorney General of Canada informed Commission counsel that the Government would not be asserting any claim of privilege in connection with the audit report. Almost a year and a half after the original request, the Government agreed to the release of the audit report in its entirety, with no redactions.

Counsel for the victims' families were able in March 2009 to provide very helpful written submissions to the Commission regarding this and other tardily disclosed documents, and these submissions were then published on the Commission's website. However, the fact remains that because of the time the Government took to respond to the Commission's request, and to come to a final position about its privilege claim, a key document, that could have been made public prior to the close of the hearings, was not available at a time and in a manner that would have allowed the issues it raised to be dealt with in public hearings.

2.3.6 Representation of Government Agencies

The Attorney General of Canada asked for and was granted Party Standing to act on behalf of the Government of Canada and all affected Government departments and agencies.[114] The Government chose to have only one set of counsel represent all potentially affected departments and agencies, as well as the Government itself.[115]

This means that, as a practical matter, the Attorney General of Canada acted for and attempted to represent the interests of the following:

(a) the Government that called the Inquiry and that asked for the answers to seven mandate questions in the Terms of Reference, mainly touching on the effectiveness of past and/or current practices by government agencies;

---

114 *Ruling on Standing*, August 9, 2006 in Annex A of this Volume.
115 *Ruling on Standing*, August 9, 2006, p. 4 in Annex A of this Volume.

(b) the government agencies whose past and present actions and practices were put in question by the Terms of Reference in circumstances where historically there had been differences and disagreements among these agencies in connection with those activities and practices;

(c) present and past individual employees of the Government and its various agencies who had historically participated in the events and activities that are invoked in the Terms of Reference, in circumstances where some had in the past been critical of Government actions or of other agencies;

(d) individual present and past employees of Government and its various agencies who qualify as experts able to provide opinions on activities and practices referred to in the Terms of Reference;

(e) the Minister of Justice, who is responsible for the conduct of the justice system in response to the unique challenge of terrorism prosecutions as referred to in the Terms of Reference;

(f) the Attorney General of Canada as Chief Law Officer of the Crown, whose constitutional duty it is to see to it that the affairs of Government are conducted in accordance with the law and the Constitution of Canada.

In explaining the decision to have all these interests represented by the same set of counsel, counsel for the Attorney General of Canada stated that the Government of Canada would "…attempt to speak with one voice" at this Inquiry, and that it had taken into account the possibility of conflicts.[116]

As a matter of principle, the intricate balancing act that would be necessary to be all things to all these people seems unlikely to be capable of meeting with any measurable success. In practice, such forebodings were amply borne out by the consequences of this unified representation at this Inquiry

It was a foreseeable result of this approach, as had been the case in the Arar Inquiry, that "…when departments or agencies had differences in positions, those differences were not explored by Government counsel."[117] Further, since the vast majority of past and present Government employees who testified before the Inquiry were represented by Government counsel, interagency differences were also not explored by counsel for Government witnesses.

A large portion of the evidence heard in this Inquiry, especially that relating to the investigation that followed the bombing, related to difficulties in interagency

116 Submissions by Barney Brucker, Transcripts, July 18, 2006, p. 3.
117 *Arar Report*, p. 291. The same approach had been adopted by the Government in its response to the Arar Commission.

cooperation, in particular between the RCMP and CSIS. Evidence of significant disputes and disagreements between CSIS and the RCMP in the course of the Air India investigation was heard, and the facts surrounding these events were examined in detail. It was clear from some of the testimony heard and mostly from the documentary record, that these two agencies had, at least in the past, taken markedly different and diverging positions with respect to the significance of the issues at stake and the very facts surrounding the disputes.[118] Given the clear differences of views between CSIS and the RCMP, the Commission would have benefited from having the evidence presented by witnesses from one agency tested by counsel representing the other agency. While the evidence in this Inquiry was heard in public, and Parties with interests different from those of the Government agencies were present,[119] the agencies would no doubt have been in the best position to vigorously test and challenge some of the evidence related to matters in which they were directly involved and of which they had first-hand knowledge. That was obviously not the approach taken on behalf of Government at this Inquiry.

Commission counsel were able to explore some of the interagency differences, but were limited because of their duty to lead evidence in an independent and even-handed manner.[120] While Commission counsel did find it necessary at times to take a more active role as a result of the challenges associated with the redaction reconsideration process, and in light of the unified representation of all government agencies, they could not advocate vigorously for the position of one particular agency in order to test and contradict the claims of another agency, and they should not have been expected to perform this function.

Although public inquiries are not "…strictly speaking, an adversarial process", in general, the Commissioner "…has the advantage of hearing evidence tested through cross-examination by those with competing points of view."[121] Having parties with divergent and opposing interests testing the evidence and making representations before the Inquiry about the interpretation of documents and testimony allows the Commission to benefit from a broad range of views before coming to its own conclusions based on the evidence. Because of the Government decision to "speak with one voice", vigorous testing of the evidence respecting interagency conflicts was made more difficult and the evidence was much less revealing.[122]

---

118 See Volume Two: Part 2, Post-Bombing, Chapter V, The Overall Government Response to the Air India Bombing.

119 In the Arar Inquiry, Commission counsel had to be instructed to cross-examine Government witnesses in order to ensure that their evidence could be tested, since much of their evidence was heard *in camera*, with no parties with interests different from the Government's interests present or represented and with one team of counsel representing all Government agencies: *Arar Report*, p. 291.

120 *Arar Report*, p. 292.

121 *Arar Report*, p. 292.

122 It is not for this Commission to pronounce on the existence of a conflict of interest between the agencies which would have made representation by the same counsel impossible. That is a matter properly addressed by the agencies and the Government within the confines of the solicitor-client relationship. The present comments are meant only to address the impact on the Inquiry process of the Government decision to have all agencies represented by the same counsel.

Further, also because of the Government decision to speak with one voice, the Commission was not presented with a clear statement of the agencies' official positions about contentious issues. At times this unified representation had an impact on the Commission's ability to evaluate factual issues. To take one clear example, in the past CSIS had alleged that the RCMP had used its information without authorization in an application to intercept private communications in connection with the Air India investigation,[123] even though in the application the RCMP claimed that such authorization had been granted by CSIS.[124] Though conflicting evidence was heard about this issue, the Final Submissions of the Attorney General of Canada provide no indication of the current position of the agencies. In fact, it is even difficult to ascertain the Government's ultimate position on this issue, as conflicting statements are made in different sections of the submissions.[125] As a result, the Commission has not been advised whether the conflict between the RCMP and CSIS positions has now been resolved and, if so, how.

More importantly, the Government's position about issues central to the Commission's mandate, such as interagency cooperation and the use of security intelligence as evidence, remains unclear, again because of the contradictory statements made in the Final Submissions. On the one hand, the Attorney General of Canada points out that current cooperative efforts by CSIS and the RCMP will not resolve the legal difficulties associated with the use of intelligence as evidence, clearly implying that change is necessary to improve interagency cooperation.[126] On the other hand, the Attorney General of Canada argues that neither disclosure law nor the *Canada Evidence Act* provisions providing for the protection of sensitive information should be modified in any way.[127] If it is the case that government agencies have different positions on those issues because of their different roles and expertise, it would have been helpful for the Commission to receive clear statements and explanations of the agencies' positions, rather than being presented with contradictory submissions on behalf of the Government as a whole.

It should also be noted that the general message contained in the Attorney General of Canada's submissions on the policy issues raised by the Terms of Reference appears to be that the *status quo* has successfully met all of the relevant policy challenges, that no changes are advisable or that any changes

---

123 Exhibit P-101 CAA0609, p. 17, where CSIS indicates they have "no record" of being told in advance by the RCMP when their information was used in a September 1985 affidavit.

124 Exhibit P-101 CAA0324(i), para. 49.

125 On the one hand, the Attorney General points out that "…whether due to a miscommunication or not, [RCMP] officers understood they had permission from Joe Wickie [a CSIS employee] to use the CSIS material in the Affidavit" [Final Submissions of the Attorney General of Canada, Vol. I, p. 132, fn 398], and on the other hand, the Attorney General indicates that CSIS Headquarters had not authorized the use of its information in the affidavit and that "…it is possible that [CSIS] BC Region had indicated a willingness to obtain permission from [CSIS] HQ on behalf of the RCMP" [Final Submissions of the Attorney General of Canada, Vol. I, para. 368]. The Government does not specify whether it takes the position that there was, in fact, a miscommunication, nor discuss whose understanding was correct.

126 See Final Submissions of the Attorney General of Canada, Vol. I, paras. 449-452.

127 See Final Submissions of the Attorney General of Canada, Vol. III, paras. 101-113.

would be premature, except for a limited number of witness protection issues.[128] This position is difficult to square with the Attorney General of Canada's role as representing the Government that called the Inquiry with the ostensible purpose of soliciting advice on addressing what it considered to be difficult but pressing policy challenges. It is somewhat surprising in that context to be told by the Government's lawyers that there is little if anything that can or should be changed.

This raises an additional important issue: what exactly is being referred to as the "Government" that is attempting to speak with one voice? The Commission is obviously not entitled to go behind issues of representation by counsel and for that reason in this chapter references to "Government" are intended to designate the originator of the instructions acted on in the context of this Inquiry by the Attorney General of Canada through its lawyers. Based on the experience of the Commission, this "Government" in fact consists of the accumulation of positions and institutional interests of the departments and agencies that played or continue to play a role in the Air India narrative. The inability of this "Government" to speak consistently, or at times at all, when these institutional interests diverge suggests that there is no single directing mind speaking on behalf of what most people would understand as the "Government." In this respect, the situation resembles that described in Volume Three, where Canada's anti-terrorism response appears to consist of the sum of the efforts of individual departments, agencies and institutions, each of which largely continues to operate "independently" (which often means within its own silo) and without overall direction.

There certainly did not appear to be any overall direction or "whole of Government" perspective in Final Submissions on behalf of the Government that suggested to the Commission that had been created by the Government to advise it about necessary changes to practice and procedure or to the operation of institutions, that no changes were needed to the legal and procedural *status quo*. Nor did there seem to be much coherence between the request of the Government that constituted the Commission to advise it of possible shortcomings in the behaviour of departments and agencies in both the pre-bombing and post-bombing eras, and the positions adopted at this Inquiry by the Attorney General of Canada on behalf of the Government which involved a systematic and consistent denial of any mistakes or deficiencies on the part of the Government agencies involved.[129] It will also not escape the notice of the reader that there is an added ironic dissonance between, on the one hand, the suggestions in the Attorney General of Canada's submissions that the Commission should avoid assigning blame and reevaluating past decisions in detail with the benefit of hindsight[130] but should rather concentrate on its

---

128 Final Submissions of the Attorney General of Canada, Vol. III, paras. 81, 100, 101-113, 115, 176, 197, 207, 244-245.

129 See Volume Two: Part 2, Post-Bombing, Chapter V, The Overall Government Response to the Air India Bombing.

130 Final Submissions of the Attorney General of Canada, Vol. I, paras. 18-19; Opening remarks by Barney Brucker, Transcripts, vol. 15, February 19, 2007, p. 1386.

mandate to provide "forward looking recommendations" to avoid problems in the future,[131] and, on the other hand, the submission of the Attorney General of Canada that nothing at this present time is in need of change.

It is also worth noting that where the Report, and especially this chapter, refers to the "Attorney General of Canada", the intended denotation is the entity that carries out the instructions formulated by the "Government" that is trying to speak with one voice. It is not intended to refer to one individual, but rather to an institutional function. Any comments about the "Attorney General of Canada" or its submissions are not intended to reflect on the personal conduct, ethics or integrity of the individual lawyers in the Department of Justice through whom the Attorney General of Canada provided legal representation in the proceedings of this Inquiry. To the contrary, it must be emphasized that these individuals conducted themselves throughout with admirable integrity and professionalism in often stressful circumstances as they did their best to discharge what to the Commission appears to be an almost impossible assignment given the disparate interests of their "unified" client.

There is no doubt that agencies, no less than individuals, are entitled to representation by counsel who will present their actions and represent their interests in their best light. Where one set of counsel is appointed to do this for a variety of agencies with historically divergent perspectives and understandings, the task becomes unmanageable and risks trivializing the real differences that separate the agencies and compromising the benefits that might be expected from the separate representation of competing viewpoints.

2.3.7 Ongoing Investigations

The criminal investigation into the bombing of Air India Flight 182 continues to this day. As a result, the Commission had to ensure that no information would be made public in the process of the Inquiry that could in any way jeopardize the ongoing investigation. While the families had been waiting too long to receive answers and the Commission therefore had to do everything possible to provide those answers, the families and the Canadian public also have an interest in seeing those responsible for the Air India bombing finally brought to justice. The Terms of Reference recognized this through a requirement that the Inquiry be conducted in a manner that did not jeopardize ongoing criminal investigations or proceedings.[132]

It was inevitable that in the course of the document collection and witness interview process, some information would be learned that might potentially have an impact on the ongoing criminal investigation. Commission counsel were instructed to exercise the utmost care in this respect, and to ensure that the ongoing investigation would not be jeopardized as a result of any new information made public in the context of the Inquiry. It was also important

---

131 Final Submissions by the Attorney General of Canada, Vol. I, paras. 1, 20, 248; Opening remarks by Barney Brucker, Transcripts, vol. 15, February 19, 2007, p. 1386.

132 P.C. 2006-293, para. (q).

that information that may have otherwise already been public not be used in a manner that could jeopardize the ongoing investigation. Commission counsel worked with Government counsel to find creative solutions to allow for the information necessary to fulfill the Commission's mandate to be made public without revealing information that could, if disclosed, negatively affect the investigation. In some cases, where focusing on certain episodes or events might arguably have risked interfering with the investigation, it was possible to lead evidence about different episodes to illustrate the same issues. At other times, it was possible to remove some sensitive details and identifying information, or otherwise generalize information, whether already in the public domain or not, in such a way that the relevant point was made without disclosing details or linkages in a manner that might have a negative effect on the investigation. As a result, the challenges associated with the parallel existence of an ongoing criminal investigation and a public inquiry were, in the end, capable of being overcome.

Nevertheless, one area of concern did arise when it was learned that on several occasions, specific aspects that the Government or its agencies characterized as part of the ongoing investigation only began to be actively pursued *after* Commission counsel made inquiries on the subject. Another serious concern arose when additional redactions were sought on the basis of what was described as a risk of jeopardizing a new investigative avenue that had just been opened when an important individual, Mr. G, contacted the RCMP to offer cooperation. In fact, Mr. G had contacted the RCMP to indicate that he wanted to testify at this Inquiry. The RCMP began discussions with him and asked him to postpone his plans to make direct contact with the Inquiry. Instead of advising the Commission that Mr. G wanted to testify, the RCMP invoked his offer of cooperation to attempt to shield information from public disclosure.[133]

However, bringing those responsible for the bombing to justice must always remain a priority, and every possible avenue of investigation should be explored, regardless of the timing or the reasons for the initial probing. Thus, the Commission continued to adopt the same general approach of avoiding the release of any information that might compromise the investigation, no matter when – or why – any specific aspect of the investigation commenced.[134]

While the imperative not to interfere with any aspect that the RCMP identified as part of the ongoing investigation inevitably leaves some loose ends and unexplored possibilities, on the whole it was possible to obtain and make public the information necessary to fulfill this Inquiry's mandate without jeopardizing the investigation. Where this was not possible, other information was found to illustrate the same themes and issues. At all times, the Commission attempted to remain mindful that its role was to address seven specific historical and policy issues, not to "solve" the bombing of Air India Flight 182.

---

133 See Volume Two: Part 2, Post-Bombing, Chapter V, The Overall Government Response to the Air India Bombing.

134 The Commission did not attempt to discover whether Commission counsel's inquiries had any impact on the decisions to begin to pursue certain aspects of the investigation at particular times.

2.3.8 Witness Interviews

To ensure that potential Government witnesses would be as candid as possible in interviews with Commission counsel, it was agreed that the interviews would remain "off the record" and confidential. It was therefore understood that the statements made by the witnesses during those interviews would not be put to them during their testimony in the hearings and that those statements would not be revealed to third parties by Commission counsel. It was felt that this approach would be conducive to making as much information as possible available to Commission counsel. Understandably, some potential witnesses would feel more comfortable in private and could freely express some personal views or share anecdotal information respecting personal interactions which they would not feel comfortable revealing in public hearings. The airing of such information and opinions in public might not have been strictly necessary to fulfill the Commission's mandate. Nonetheless, it was felt that this added context would better position Commission counsel to evaluate the evidence that did need to be called and to understand the significance of the information contained in the documents collected.

Overall, this approach was successful in making more information and context available to Commission counsel. However, in some cases, Government witnesses not only avoided repeating the opinions previously expressed in interviews, but actually presented contrary and incompatible opinions or positions while testifying in the public hearings. Because of the initial agreement with Government, Commission counsel were prevented from exploring the reasons for the change of views on the witnesses' part or from probing further into possible differences between the institutional positions of the Government or its agencies and the opinion of individuals working within those institutions. This raised particularly serious concerns in connection with the evidence relating to the current regime for national security investigations and to the current level of interagency cooperation. Documentary or other evidence that might provide additional information or background was not generally available with respect to those matters, in light of the risk of compromising ongoing investigations or operations. As a result, the contradictions between opinions expressed in interviews and in public hearings, and the apparent incompatibility between institutional positions and personal views, remained largely incapable of exploration.

None of the statements made by witnesses in interviews have been used as the basis for any of the conclusions or recommendations in the Report, and the content of these statements will remain confidential. However, since the initial agreement with Government was not meant to allow witnesses to present different and incompatible versions of events without explanation, the advice of Commission counsel respecting blatant incompatibilities between the interview statements and the public evidence was considered relevant to

the assessment of the degree of reliance that could be placed on the evidence respecting certain matters.[135]

2.4 Conclusion

In the end, it was possible to fulfill the mandate of the Commission and to inquire into all of the matters set out in the Terms of Reference. It did prove possible to conduct the Inquiry in accordance with the principles of thoroughness, fairness and independence, as well as in accordance with the fundamental principles of openness and transparency. However, as a result of the factors discussed above, the process was not always as expeditious as initially had been hoped.

All those who were involved in the Inquiry faced significant challenges and all, including Commission counsel, at times made errors in their sincere but unrealistic attempt to meet ambitious deadlines that were intended to give the public, and especially the families, the timely answers they deserved. The procedural challenges encountered in the Inquiry often – but not always – resulted from positions taken by the Government agencies involved, especially with respect to NSC claims. This by no means implies any bad faith or misconduct on the part of the Government counsel who appeared before this Inquiry. On the contrary, Government counsel acted honourably and seemed to attempt to the best of their abilities to carry out their instructions in a manner that recognized their ethical and professional obligations. Wherever responsibility for some of the problems outlined in this chapter might lie, it should not be laid at the feet of the diligent individuals who consistently strove to represent their clients as well as was possible under extremely difficult circumstances.

Despite the difficulties and setbacks, the most important objectives of the Commission were accomplished with the cooperation of all Parties and counsel involved. In the end, it was possible to hold the Inquiry hearings in public and to provide answers that can at last be openly shared with the families and with the Canadian public.

---

135 The Government, having been made aware of concerns about specific contradictions between witness interviews and certain portions of the evidence presented before the Inquiry, nevertheless chose to rely on such "contradicted" evidence in its final submissions in at least one instance.

VOLUME ONE
THE OVERVIEW

CHAPTER III: HISTORICAL

3.0 Pre-Bombing: Assessment and Response to the Threat

As stated, the Air India Flight 182 tragedy was the result of a cascading series of failures. The failures were widely distributed across the agencies and institutions whose mandate it was to protect the safety and security of Canadians. There were structural failures and operational failures; policy failures, communications failures and human errors. Each contributed to, but none was the sole cause for, Sikh terrorists being able to place a bomb in the checked baggage loaded aboard Flight 182 without being detected. Some failures came to light almost immediately, but a number have lain undetected, or at least unacknowledged, for decades and have only come to light during the currency of this Commission of Inquiry.

The first question posed by the Terms of Reference of this Inquiry is whether Canadian institutions adequately understood and assessed the threat posed by Sikh extremism.

All of the institutions and agencies were theoretically aware of the potential threat to safety and security posed by terrorism in general. A few had some knowledge of the dangers of its Sikh extremism version in particular. Several were nominally aware of the threat of sabotage to passenger aircraft by means of timed explosive devices in checked baggage, and one agency was even aware of information indicating that Air India might be targeted by this method in June 1985. As a practical matter however, none of the institutions or agencies was adequately prepared for the events of June 22/23, 1985.

Indeed it is impossible to draw any conclusion other than that, almost without exception, the agencies and institutions did not take the threat seriously, and that the few individuals within these institutions who did, were faced with insurmountable obstacles in their efforts to deal with the threat.

There are a number of plausible ways to break down the failures that allowed the bombing of Flight 182 to occur. Each of the agencies and institutions that should have had a role in preventing terrorist attacks displayed structural flaws that impaired their performance in:

a) detecting the threat
b) assessing the threat, and
c) putting in place reasonable counter measures to respond appropriately to the threat.

While each institution must be understood in terms of its own unique circumstances, there are general themes that weave their way through all the separate parts of the story.

3.1 Intelligence and the CSIS Investigation

The intelligence community has the primary responsibility for anticipating threats to national security. The primary responsible agencies at the time of the terrorist attack on Flight 182 were the Canadian Security Intelligence Service (CSIS), whose mandate is to collect, analyze and report information about threats to Canada's security, and the Communications Security Establishment (CSE), which monitors foreign electronic communication to provide intelligence to the Government of Canada and its agencies.

CSIS only came into being as an independent civilian agency in 1984. Before that, the national security intelligence was under the purview of the Security Service of the Royal Canadian Mounted Police. The circumstances surrounding the birth of CSIS had a deep and detrimental impact on its ability to detect the particular security threat posed by Sikh extremism and on its ability to provide useful advice to the agencies and institutions charged with protecting Canadian lives and property.

Although the notion that intelligence should be handled by a civilian agency rather than the police had been widely discussed and debated in Canada for over a decade, the *CSIS Act*, which brought about this transformation, was passed hurriedly as the last legislative act of the outgoing Liberal government in June of 1984. It was then left to be implemented in a very short time frame by a new Progressive Conservative administration with limited accumulated experience in the area of national security. The result was an uneven transition, marred by scarce resources and by bruised feelings: both at the RCMP, which felt wronged by the removal of its intelligence mandate, and at CSIS, which felt poorly supported in its new role.

While intelligence officers were aware of the existence of the phenomenon of Sikh extremism, the rise in the intensity, fervour and potential danger of this phenomenon was the result of events in the Indian sub-continent that took place in the same time frame as the transition from the Security Service to CSIS. These events included the occupation and fortification of the Golden Temple in Amritsar, Sikhism's central shrine, by armed Sikh separatists, the subsequent bloody storming of the Golden Temple by the Indian army, and the resulting massacres and intercommunal violence in the State of Punjab, all of which

culminated in the assassination of Indian Prime Minister Indira Gandhi by her own Sikh bodyguards. This chain of events led to a rise in anti-Indian sentiment within the Sikh diaspora, including the Sikh community in Canada.

Even in a relatively stable institutional environment, keeping up with the rapidly changing landscape of Sikh extremism in Canada would no doubt have proved challenging. The impact of the transition from the RCMP Security Service to CSIS made a difficult situation that much worse.

Although CSIS personnel were dedicated and hardworking, the institutional context was poorly geared toward dealing with terrorism in general – and with a terrorist threat arising from Sikh extremism in particular. Canadian intelligence gathering was stuck in a Cold War paradigm in which the primary threat to national security was assessed as emanating from espionage by hostile foreign governments. Most resources were allocated to counter-espionage, with comparatively few resources devoted to counter-terrorism.

Of the resources devoted to counter-terrorism, most were concentrated on the risks posed by Armenian terrorist attacks against Turkish interests in Canada. Even at the so-called "Sikh Desk" at CSIS headquarters, (which was a sub-unit of the "Western Europe and Pacific Rim" unit of the Counterterrorism unit) the arguably inadequate official complement, consisting of a unit head and four analyst positions, was in fact only partially staffed. Only the unit head and two analyst positions were actually filled, and that even smaller number was further reduced by the fact that, for the better part of the year leading up to the bombing of Flight 182, one of the incumbents was away on French language training. In the Regions, staffing was equally thin. In BC Region, where the most militant and most obviously dangerous elements of Sikh extremism in Canada were to be found, two investigators were responsible for the entire investigation of Sikh terrorism.

CSIS personnel assigned to this investigation received no additional training; investigators and analysts were expected to learn on the job.

CSIS appears to have uncovered little, if any, information on its own, with most of its information coming from the Government of India through the Indian High Commission. The full extent of CSIS's knowledge in the summer of 1984 was that Talwinder Singh Parmar had been released from prison in Germany following a failed extradition attempt on murder charges by the Government of India, and had returned to Canada, where he was launching a public campaign of fiery rhetoric and communal intimidation to radicalize gurdwaras (Sikh temples) and to take over their direction and their revenues. CSIS was unable to provide confirmation of its existence in Canada, let alone the actual size of the extremist Babbar Khalsa movement that Parmar claimed to lead, and even referred to it as the "Barbara Khalsa group." By the fall of 1984, CSIS had pieced together enough information to be able to identify Parmar as the most dangerous Sikh in Canada and to opine that his associate Ajaib Singh Bagri could be manipulated to carry out a terrorist attack.

Despite its awareness of the threat and of the identity of the potential protagonists who might carry it out, CSIS appears to have obtained little important new information of its own about the Sikh extremist threat or about the Babbar Khalsa or about Parmar from the fall of 1984 through to March of 1985. The major reason for this gap lay in the state of the warrant approvals process that had been put in place by the *CSIS Act* in June 1984.

On the ground, CSIS BC investigators were aware of the urgent nature of the threat from Sikh extremism and of the inadequacy of their information resources to deal with it. They simply had no information sources of their own and had been totally unsuccessful in recruiting sources within a Sikh community that was somewhat insular and vulnerable to intimidation by the extremists. They soon concluded that they needed surveillance and electronic intercepts in order to be able to understand and respond to the increasing threat.

The institutional response to the request to approve a warrant to intercept Parmar's communications demonstrates a fixation with form over substance and, despite protestations to the contrary at the time – and subsequently, suggests a lack of appreciation of the reality of the threat.

The civilianization of CSIS was in part a reaction to RCMP Security Service excesses in its investigation of the Front de Libération du Québec (the "FLQ") and extremist Quebec Separatists. Under the RCMP Security Service, while electronic intercepts had required approval, the process was informal, simply requiring a request to the Solicitor General, the Minister responsible for the RCMP (and later also for CSIS). With the creation of CSIS, as one of the means to protect civil liberties from unjustifiable intrusion by or on behalf of government, a new system of judicial supervision of certain intelligence operations was instituted, including a requirement for judicial approval for intercepting private communications. This new protocol was to apply prospectively but also was intended to cover existing intercepts that had been approved by the Minister. There was an explicit requirement that existing intercepts had to be reviewed internally and approved by the Solicitor General and then by a judge of the Federal Court, all within 6 months of the coming into force of the *CSIS Act*, i.e. by January 1985.

When added to the considerable stresses and strains that accompanied the rushed transition to CSIS from the RCMP Security Service, it was entirely foreseeable that this warrant conversion process would be the source of added pressure and potential misadventure. The foreseeability of the problems that might be caused by the requirement to devote considerable resources to the conversion process should have called for added care and attention to ensure that the process would be capable of meeting new needs that would arise and not just of preserving existing arrangements. Instead, the response of CSIS was to prioritize existing warrants and to defer new applications, with the exception of only those deemed most urgent. As CSIS understandably would want to avoid disrupting existing investigations, in theory, this process could be considered a

sensible policy; in practice, its effectiveness depended on the Service's ability to respect the new needs that were more urgent.

The evidence before the Commission indicates that, despite the priority afforded to the warrant conversion process, it was possible to secure a warrant in an extremely short timeline to respond to a perceived urgent priority, as occurred in an area other than the threat of Sikh extremism. The protracted wait for the processing of the Parmar warrant application either demonstrates an unthinking application of the concept of priority of existing warrants or, more likely, reflects the lack of appreciation of the true urgency of the threat of Sikh extremism.

Despite certification by the existing chain of command in BC as well as by the Headquarters counterterrorism hierarchy, and despite increasingly pointed memoranda from the front lines in BC, the application for the Parmar warrant lay dormant for months while the conversion process went forward. Then, after proceeding through multiple steps in the complicated, and still in flux, approval process, it was further delayed for an additional month by what turned out to be an irrelevant issue raised by the Minister's Office. Although the final steps leading up to the submission of the warrant to, and approval by, the Federal Court proceeded relatively quickly, the total time from the request for a warrant to the date of approval was over five months. This lengthy delay was entirely disproportionate to the heightened threat and the demonstrated lack of intelligence sources available to respond to it.

The subsequent course of the BC investigation confirms the theme of inadequate resourcing and indicates that execution on the ground was not sufficient for the seriousness of the threat being dealt with.

Eventually the BC investigators did get approval both for electronic intercepts and for physical surveillance coverage on Parmar. As will be seen, the story of neither effort is particularly edifying.

3.1.1 Physical Surveillance

The mobile surveillance of Parmar was carried out for 39 of the 72 days: between April 6 to June 16, 1985, including continuously for the first two weeks of June 1985 – an exceptionally long period for what was seen as a very scarce resource. Nevertheless, as has been widely reported, this surveillance was withdrawn on June 17, at precisely the most crucial time in terms of the terrorist preparations for the bombing. The stationary observation post (OP) near Parmar's residence was also withdrawn on the day of the bombing. The rumour that the OP withdrawal was to allow the investigators to participate in a social event appears to be based on a misunderstanding of the CSIS code name for the operation to which the surveillance team was reassigned. Nevertheless the fact that surveillance was redirected to shadow a counter-espionage target at the moment when the danger of an act of domestic terrorism was at its height, is a telling illustration of how poorly understood the threat was.

No less telling is the way the surveillance was conducted, and especially how it was (or was not) used. The conduct of the surveillance was marked by numerous low lights, with the surveillants unable to keep track of their targets, and often mistaking one traditionally-attired Sikh for another. This apparent inability to tell one Sikh from another continued into the post-bombing era as well.

The nadir of ineffectiveness of CSIS pre-bombing surveillance is arguably the moment of what perhaps might have been its greatest success: the monitoring of the "Duncan Blast." On June 4, 1985, a CSIS surveillance team followed Parmar as he traveled with a young man, misidentified by the surveillance team as Parmar's son Jaswinder, to the BC Ferry Docks. The lead surveillance car narrowly avoided missing the ferry, a fate the second car and its surveillance team was unable to avoid. The lead surveillance team followed Parmar's car to the Duncan, BC residence of Inderjit Singh Reyat, who would later be convicted of manslaughter for his role in the Narita, Japan, bombing, and would enter a guilty plea in connection with the terrorist attack on Flight 182. The surveillants followed Parmar's car from Reyat's house to a clearing off the highway in the woods near Duncan and saw Reyat and Parmar walk into the woods. Shortly thereafter, they heard a loud explosive sound coming from the woods which they misidentified as a shotgun blast. The team observed Parmar and Reyat emerge from the woods and put something in the trunk of Parmar's car. They then followed the car to Reyat's residence where the young man got out of the car and accompanied Reyat into his house.

Although they were on a surveillance mission, the surveillants did not have a camera and so were unable to photograph the unknown young man, who would later be referred to as "Mr. X." This individual was the subject of a long and unsuccessful search to discover his identity as one of the missing pieces in the Air India narrative. Although they remained on Vancouver Island for the night, the surveillants were, for unknown reasons, unable to secure permission to follow the young man the next day and thus lost a further chance to make the crucial identification.

Additional examples of such fumbling extended into the post-bombing investigation of the identity of Mr. X. When the RCMP obtained school records placing Parmar's son Jaswinder in school on the day of the Duncan Blast and began to raise questions with CSIS, CSIS did nothing to verify whether its team had misidentified the person accompanying Parmar and Reyat. In fact, even when one of the CSIS surveillants who had followed Parmar and his associates to Duncan began to work for the RCMP and, having there the opportunity to view Jaswinder at close range, realized with certainty that he was not the person she had seen on June 4th, CSIS still stubbornly maintained that Mr. X was Jaswinder. CSIS did not question the PSU team in light of the RCMP's expressed concerns. Even a cursory review of its surveillance records pertinent to this issue would have revealed that its surveillance team placed Jaswinder in two places at the same time: on Vancouver Island and at school in Vancouver on the day after the Duncan Blast.

In addition to the failure to identify Mr. X, there were further investigative dead ends resulting from the mis-transmission in the CSIS Report of the telephone number Parmar was seen to have dialed from the ferry.

Even the most important achievement of the surveillance, hearing the explosion in the woods, was marred by the misinterpretation by the surveillants of what they actually heard. The surveillants thought they heard a shotgun blast, when in fact they heard an explosion intended to test the detonation system for the bombs Parmar was building. Instead of leading to a realization that Parmar was planning to blow something up, the surveillants' belief that they heard a gunshot supported the mistaken conclusion by the CSIS BC Region that the primary danger from Parmar and the Babbar Khalsa was a possible assassination attempt or armed assault. But even this misinterpreted information, which at the very least appears to demonstrate that Parmar and his group posed a serious threat to commit a terrorist act, never made it into the formal CSIS threat assessment process. Likewise, a number of other significant pieces of threat information in various hands were also never reported, further compromising the ability of the CSIS HQ threat assessment process to put together the pieces of the puzzle in time to raise an effective response to the threat that was to crystallize into the terrorist attack on Flight 182.

3.1.2 Electronic Surveillance

The fate of the electronic surveillance on Parmar, finally approved in March 1985, was no less problematic, and arguably constituted an even more serious failure because of its consequences for the subsequent investigation of the bombing.

In this case too, resource issues were important. While listening devices can record conversations, it takes human resources to transcribe, to translate if necessary, and, ultimately, to analyze and interpret them. Each of these steps proved problematic. In order to safeguard security, CSIS, like the RCMP Security Service before it, adopted stringent security qualifications for its translators, including lengthy periods of Canadian residency as well as Citizenship.

As prudent as this may have seemed in the abstract, in practice it meant that there was only a very small pool of potential translators available for recruitment. In BC Region it meant that there were no Punjabi translators available at all. To cope with this problem, the tapes of the Parmar intercepts were shipped to Ottawa, where they were added to the workload of the already overburdened Punjabi translator at CSIS Headquarters. Delays were inevitable and a serious backlog ensued.

Shipping the tapes across the country meant that there was no meaningful possibility for the BC investigators to interact with the translator, who was essentially left to her own devices to extract, translate and summarize what was related on the tapes. Although a Punjabi translator for the BC Region was eventually recruited and began work on June 8, 1985, a significant backlog of translation work in BC remained throughout the pre-bombing period. There still

seems to have been little interaction with the investigators on the ground and there remains some doubt as to how many, if any, of the "transcripts" that were produced were in fact reviewed by the investigators.

The transcripts were prepared by a transcriber who reviewed and summarized what she thought relevant in the English language content, adding material from the Punjabi content based on the translators' notes. The effectiveness of this disjointed process became further impaired by the vacation schedules of the transcriber and one of the investigators. One of the investigators was off duty in the two weeks leading up to the bombing and the transcriber was away just prior to, and for a week after, the bombing. Because the intercept tapes were erased shortly after they were processed, there was no opportunity to go back to the actual tapes for further analysis or to remedy any deficiencies in the transcription and translation process. Whatever information was not recorded in the transcription notes was lost permanently.

As discussed elsewhere in this Overview, disputes remain as to the actual content of the tapes that were reviewed and of those that were caught in the backlog, as well as about the adequacy and comprehensiveness of the review and analysis. What is beyond doubt is that no material from the Parmar intercepts made its way into the CSIS, or any other, threat assessment process in April – May or June of 1985.

3.2 The RCMP Response

In a Cold War environment, it was possible to conceptualize the worlds of intelligence gathering and law enforcement as being entirely distinct, and each function as better off divided from the other. The intention of the drafters of the *CSIS Act* was to separate the two functions. The idea was that CSIS would have a monopoly on intelligence gathering and the RCMP would have a monopoly on assembling evidence. CSIS would be proactive, attempting to anticipate security risks, while the RCMP would be reactive, responding to crimes and attempting to bring the perpetrators to justice.

Reality did not unfold in conformity with those early expectations. In the post-bombing period, and to the present day, the major stress on the original model would turn out to be the assumption that CSIS intelligence information would have no role to play in court proceedings or in the criminal justice system. In the pre-bombing era and immediately thereafter, however, the main area of contention between the agencies was precisely about CSIS's presumed monopoly on intelligence gathering and assessment.

In part, this was a function of an unwillingness by the RCMP to let go of the notion of a unified investigative effort and of intelligence-gathering resources as a "Special Branch" of the RCMP. It also related to a perceived "gap" created when the Security Service was separated from the Force. The RCMP believed that CSIS intelligence gathering and its threat assessment process would not be sufficient to address the "criminal perspective" and that it would not be

able to make good use of the threat information incidentally obtained by the RCMP members in the conduct of their regular policing duties. These views found expression in the notion that the police needed "criminal intelligence" as distinct from the "security intelligence" gathered by CSIS. This notion was given a huge boost by the *Security Offences Act*, which was passed as Part IV of the Original *CSIS Act* and which specified that the RCMP mandate was to include the investigation of crimes that were "Security Offences."

In fact, the *Security Offences Act* merely gave the RCMP jurisdiction to investigate criminal cases that would have traditionally fallen under the responsibility of provincial or municipal police forces in locations where the RCMP was not the police of jurisdiction. The RCMP, however, read more into the new provisions. Rather than depend on CSIS to provide for its intelligence needs, as intended in the 1984 Ministerial Directive issued by Solicitor General Robert Kaplan, the RCMP posited a relationship in which CSIS dealt with "security intelligence," but in which intelligence relevant to a "security offence" would constitute "criminal intelligence" within the purview of the RCMP mandate.

Although the RCMP's initial efforts to reconstitute a "criminal intelligence" function analogous to its lost Security Service mandate were denied funding or staffing approval, the RCMP nevertheless did manage to put together a rudimentary parallel structure designed to collect and analyze intelligence so as to allow the RCMP to engage in "threat assessment" from a "criminal" point of view.

Because of the deficiencies in the new RCMP structure and process, gaps in the threat assessment process were never adequately addressed. The structure proved incapable of addressing the pre-existing difficulties in incorporating threat information incidentally obtained by RCMP members. It also proved unable to deal with new problems that would emerge as a result of the creation of a separate civilian intelligence agency, including the difficulties down the road in using CSIS information for court purposes. The existing delay in transmitting information through cumbersome formal mechanisms for information exchange was left unaddressed, and was in fact aggravated by the new RCMP threat assessment process.

In the end, RCMP threat assessments usually contained no more, and often less, information than the assessments that CSIS, in parallel efforts, continued to produce. While the RCMP devoted resources to duplicating CSIS's work, it still managed to deprive the new agency of important information, including information that CSIS needed to assess terrorism threats.

The newly created National Security Enforcement (NSE) units were intended to identify threat information, but had neither the mandate nor the capacity to conduct investigations that might unearth such information. On the other hand, the regular RCMP units who were expected to carry out these investigations had no training or experience in dealing with this sort of threat information.

The purpose of the new RCMP threat assessment process was not clearly defined or understood within the Force. The manner in which the new RCMP functions could be distinguished from those of the CSIS Threat Assessment Unit remained unclear. RCMP members received no clear instructions as to the type of information they were expected to identify, report and share. They received no special training about the threat assessment process and the impact of the creation of CSIS on their responsibilities. As a result, the individuals involved often failed to appreciate the significance and requirements of the threat assessment function, and a great deal of relevant threat information went unreported and was not shared – even internally.

Crucial information, such as the fact that Parmar's group was working on a "highly secret project" in the spring of 1985, and the information received from Person 1 in September 1984 about the November Plot to bomb an Air India aircraft, was not reported to RCMP HQ and, hence, was not taken into account in the RCMP threat assessment process.

RCMP failures to report information internally often also meant that the information was not shared with CSIS. Where the information was not otherwise available to CSIS, it was never included in *any* threat assessment process and the RCMP Protective Policing (P Directorate) was never advised.

The manner in which the RCMP processed information it received from CSIS also created obstacles. The liaison process put in place by the RCMP generally had limited success. Information continued to be shared informally, with members of each agency relying on personal contacts in the other agency. Because of tense relations between CSIS and the RCMP in the early years in British Columbia, CSIS at times used Vancouver Police Department (VPD) members as a conduit to pass information to the RCMP. Informal and indirect sharing between agencies meant that no consistent records were created. This lack of consistent records made it difficult for the RCMP, despite its repeated attempts at file review, to locate, let alone to analyse, all relevant information.

RCMP Divisions were supposed to obtain and report threat information from local police forces, but relations between the RCMP and local forces were also often tense. The RCMP insisted on being the first and only recipient of CSIS intelligence and reserved for itself the decision to pass the information to local forces as it saw fit, often invoking as a justification the fact that most local police officers were not security-cleared.

In British Columbia, where relations with local forces were less tense, the RCMP nevertheless failed to achieve sufficient integration and information sharing. The RCMP did not sufficiently share its own information with the VPD members of the Vancouver Integrated Intelligence Unit (VIIU). The VPD members of VIIU received a great deal of information from the VPD's Indo-Canadian Liaison Team (ICLT), which had managed to gain trust in the Sikh community. But the RCMP often did not access the VPD files, or it failed to recognize the significance of the information it received from the VPD.

The RCMP E Division NCIS terrorist/extremist unit had limited knowledge of the most important players in the Sikh extremist movement and had few resources to devote to developing this knowledge. The wealth of general intelligence gathered by the ICLT about local extremist organizations was not reported to RCMP HQ. Specific information, such as the comment made by a Sikh extremist leader in mid-June 1985 indicating that something would happen in two weeks, was also not reported to HQ, and was not taken into account in the RCMP threat assessment process. As a result, the RCMP HQ branch had little or no context to allow it to understand the significance of the threat information it did receive from the Divisions.

In BC, the Criminal Intelligence Service of BC (CISBC) was available to the RCMP. The CISBC was part of a program bringing together the intelligence units of provincial and municipal police forces with that of the RCMP to exchange information. The RCMP failed to access crucial information that was part of the CISBC holdings.

The fate of the Duncan Blast information demonstrates both the impact of the failure by RCMP personnel to utilize the channels that Headquarters had attempted to establish for purposes of information sharing, and the RCMP's inability to identify and report relevant threat information. The Duncan Blast information was provided by CSIS to RCMP members in E Division, but was not shared with the RCMP liaison unit. Because the information was not internally reported to the NSE unit, it could not be disseminated within the RCMP to all the units that might have needed it. The information also did not enter the RCMP threat assessment process. CSIS did provide the information to the VPD, which in turn shared it with the RCMP during a briefing, but again the information did not make its way to RCMP HQ. A report about the information was also available at CISBC, but was not accessed by the RCMP prior to the bombing.

Because records of the exchange of information that actually took place were not kept, CSIS and the RCMP are still debating to this day the sufficiency of the information that was shared about the Duncan Blast.

The RCMP failure to provide threat information to CSIS was essentially self-defeating, since its P Directorate largely relied on CSIS threat assessments to determine what security measures to implement. In the same way, the RCMP's failure to disseminate information to its own units, or to report threat information to HQ, meant that P Directorate was also deprived of the possibility of receiving the information through RCMP threat assessments.

The lack of communication up to HQ from the Divisions was mirrored by the lack of communication down from HQ to the divisional units. The failure to provide the Divisions with information and assessments about threats to Air India greatly impaired investigations at the local level. Not only did RCMP investigations have to proceed on the basis of incomplete information, but local police units that might have been of assistance could not participate.

The RCMP reporting structure was further ill-adapted to the threat assessment process because divisional units did not report directly to HQ. The HQ branch had no direct authority to command divisional investigators and was not kept sufficiently updated about the details of ongoing investigations to be able to provide useful suggestions in any event. It was left to divisional investigators, with no national security training and no appreciation of international issues, to decide which matters to probe further, and when.

The deficiencies in this structure were particularly apparent in the investigation of the November Plot, which involved information, originally obtained from two sources in the fall of 1984, that Sikh extremists were plotting to place bombs on two Air India aircraft. The Division provided insufficient information to HQ from the start, not immediately reporting crucial facts that would allow HQ to make its own assessment of the seriousness of the threat. Instead, the Division's scepticism about the validity of the information was relayed to P Directorate; a scepticism found to be unwarranted.

The Division provided few reports about the investigation, and those it did provide did not contain sufficient information. After the bombing, the Division ignored repeated requests for updates and, for over a year, failed to provide information it had promised HQ. A HQ member eventually turned to CSIS for the information, which it received three days later. Because of the Divisions' resistance to central direction or authority, the HQ branch was totally incapable of fulfilling its mandate to gather and analyse threat information.

There were other significant deficiencies in the flow of information. Intelligence regarding threats to national security was often not transmitted to the HQ threat assessment unit (NCIB/NSE) by other RCMP branches or directorates. Although P Directorate depended on CSIS and RCMP threat assessments to carry out its own functions, it often did not transmit information about threats to Indian interests that it received from External Affairs. Airport Policing detachments often did not transmit threat information about Air India, which they received directly from the airline, to the HQ Airport Policing Branch. Even when they did, the information was often not shared with NCIB or CSIS. In the pre-bombing period, RCMP airport detachments did not send to Headquarters information that had originated from Air India about the need to carefully examine "… cameras electronic equipments and parcels carried as hand baggage," nor the information about the threat of a terrorist group intent on exploding a device on an international airline in flight by placing an explosive inside a suitcase. Since RCMP HQ was not receiving comprehensive information, it could not properly advise other airport detachments that might be affected, such as those with flights connecting to Air India.

Since information was not provided to the divisional units, it could not be shared with local police forces. When E Division reported in April 1985 that it had no information from any sources indicating that any bombing of an Air India plane would occur, NCIB did not (and likely could not) take any steps to correct this impression, in spite of the fact that there was, indeed, information about threats

to Air India suggesting that hijacking or sabotage were possibilities and that the threat to Air India was considered high.

The HQ section in charge of threat assessment and the divisional units it relied on to gather information had limited analytical capability. In British Columbia, despite a mass of information indicating significant activity by Sikh extremists, the threat was sometimes assessed as non-existent or very low. HQ NSE members often simply passed information on to P Directorate without attempting to assess it and without asking further questions. Even worse was the inappropriate substitution of credibility assessments, based on criminal law evidentiary standards, for threat assessment. The RCMP treatment of the November Plot is a clear example of this phenomenon: RCMP investigators, suspicious about the motivations of the individuals who provided information about a possible bomb plot, failed to report this information to HQ or to share it appropriately with CSIS.

The crux of the matter is that the creation of a parallel RCMP threat assessment process precluded the establishment of a single location for the centralized assessment of all of the threat information in the Government's possession. CSIS and the RCMP collected and analysed their threat information separately, with neither agency able to conduct a complete analysis of the entirety of the available information. NCIB had access to CSIS threat assessments, but did not access them or incorporate them into its own analyses. CSIS was often not provided with the information in NCIB's possession. NCIB itself did not receive all the RCMP information. RCMP P Directorate received the most information, but had no central threat assessment mandate or capacity of its own and was fully dependent on CSIS and NCIB to assess the seriousness of threats.

In the end, the RCMP proved incapable of the effective collection and reporting of even its own information. When it did report information, its significance was often not recognized.

3.3 What Was Known

Perhaps the central unanswered question that Canadians, and especially the families of the victims of the bombing of Flight 182, have hoped a Public Inquiry might reveal is whether the Government and its institutions had information prior to the bombing that could have allowed the authorities to prevent it.

The answer is complex. There is no evidence that the Government was aware in advance of the details of the events of June 22, 1985. That is the basis for the oft-repeated statement that there was no knowledge of any "specific threat" against Flight 182.

To pose the issue in this form is, however, to miss the point. In 1985, "specific threat" was a technical term tied to emergency protocols put into place when the authorities received a call-in threat that identified a target, in circumstances

where there was not enough time to conduct a proper investigation or assessment of the threat. This sort of "specific threat" justified emergency measures because of the magnitude of potential consequences even if it wasn't possible to assess the likelihood of their occurrence.

It is one thing to say that, had there been such a "specific threat," detailing a time, place and method of a planned attack on Flight 182, emergency measures would have been implemented to hunt down the bomb. It is entirely something else to suggest that, in the absence of such a detailed, precise and "specific" threat, nothing further could or should have been done to prevent the bombing.

The claim that there was no "specific threat" to the June 22, 1985 departure of Flight 182 is accurate only in a limited and literal sense. No one source provided detailed information to any one agency in one place and at one time about the plan to blow up Flight 182 on June 23, 1985. On the other hand, various agencies of government had extremely important pieces of information that, taken together, would have led a competent analyst to conclude that Flight 182 was in danger of being bombed by known Sikh extremists.

Prior to the bombing, CSIS, the RCMP, the Department of External Affairs, local police forces and Transport Canada were collectively in possession of the following information about Sikh extremism and threats to Indian interests:

- A plot to bomb one and possibly two Air India planes was allegedly being hatched by Sikh extremists in British Columbia in the fall of 1984;
- In the fall of 1984, Ajaib Singh Bagri was allegedly nominated to a committee planning the hijacking of an Air India plane;
- Talwinder Singh Parmar's group, the Babbar Khalsa, was reportedly working on a "highly secret project" in the spring of 1985, and Parmar had been assessed as the greatest threat in Canada to Indian diplomatic missions and personnel;
- In early June, Parmar and associates conducted experiments in the woods involving a loud explosion;
- During a June 12, 1985 meeting, a prominent Sikh extremist stated – in response to questions about the lack of attacks on Indian officials - that something big would happen in two weeks; and
- In late May and early June, Air India warned that sabotage attempts against Air India planes were likely to be made by Sikh extremists using time-delayed devices in registered baggage, that special vigilance was warranted on items like transistor radios, and that police should oversee the loading of registered luggage onto airplanes.

James Bartleman, who at the time he gave his evidence was Lieutenant Governor of Ontario, and in 1985 was Director General (DG) of the Intelligence Analysis and

Security Bureau at External Affairs, testified that shortly prior to the bombing, he saw, as part of the material he received electronically from CSE on a daily basis, information that indicated that Flight 182 would be targeted. He was not able to assess the reliability of the information but thought it important to ensure that the authorities were aware of the information and were dealing with it. When he brought the information to the attention of an RCMP official who was attending a security meeting in the building, he was met with a hostile reception and an indication that the RCMP was aware of the matter and had it in hand. On June 23, 1985, when he was informed of the bombing, he thought immediately that this was the materialization of the threat, and that the authorities had been unable to prevent it.

Counsel from the Department of Justice, on behalf of the Government and all its agencies, approached Bartleman's evidence as though it was the only pre-bombing indication of the danger to Air India Flight 182. In an entirely misguided approach, Bartleman was aggressively cross-examined and witnesses were called to attempt to call into question the details of his evidence.

Intelligence specialists often observe that an item of information, although apparently insignificant in itself, may in fact be the missing piece to a puzzle that helps a foreign or hostile group or agency see a pattern or draw conclusions that have profound intelligence value. This "mosaic effect" metaphor is typically used by intelligence agencies, sometimes excessively, to describe the potentially dangerous consequences that can result from the disclosure of their own information and to justify the need for secrecy. It is an equally apt description of how gathering and sharing information can help an agency's own intelligence effort.

The essence of good intelligence analysis is that it pulls together disparate facts and information from diverse sources to assemble a pattern in which one can have confidence. Once enough information has been assembled, even seemingly insignificant new additions can lead to new insights and deeper understanding.

However startling and important Bartleman's testimony may be, it is not, as the blistering assault on his credibility by some Government witnesses and the Attorney General of Canada's submissions would imply, the only evidence that suggests that the Government had enough knowledge of the threat to Flight 182 to warrant a different security response.

Even without the document that Bartleman described, there was more than enough disparate pieces of information that, had they been assembled in one place, would have not only pointed to the nature of the threat, but would have provided corroboration for the seriousness of that threat, thereby highlighting the need to implement measures aimed specifically at responding to the possibility of sabotage by means of explosive devices concealed in checked baggage.

Bartleman's evidence is best understood as simply one more piece in the mosaic.

In 1985, the institutional arrangements in place and the prevailing practices of Canadian information-gathering agencies were wholly deficient in terms of allowing the mosaic of the threat of Sikh extremism to be pieced together so as to make visible the pattern that clearly pointed to the high risk of a bombing of Flight 182.

The consequence of these deficient arrangements was that CSIS, the government agency that was given the primary responsibility for threat assessment, did not have sufficient access to facts about the threat of Sikh extremism. Lacking good access to sources of its own within the Sikh community, CSIS was heavily dependant on other agencies, both foreign and domestic, for the information it needed to understand the threat. CSIS had an abundance of threat information from the Indian government about the situation in India and about what was going on in the Sikh community in Canada, but it was unable to corroborate it. Without corroborating information, however, the large volume of information from the Government of India gave the impression that it was "crying wolf."

CSIS's lack of access to sufficiently detailed information, perhaps compounded by a lack of necessary technical skill, compromised CSIS's ability to identify the nature of the danger and to determine, with any degree of reliability, the likelihood that it might materialize. The result was the production of threat assessments that provided a qualitative assessment of the danger as "high" or "elevated," with little detail that would allow a recipient of the assessments to make intelligent decisions as to how to deploy, or how to prioritize the deployment of, scarce protective resources, which is, ultimately, the purpose of threat assessment.

In terms of the most important information regarding threats to Air India in the year leading up to the bombings, CSIS appears to have been provided with very few of the essential pieces of the mosaic possessed by other government agencies.

One of the most striking instances of the impairment of CSIS's ability to benefit from the mosaic effect is the June 1st Telex.

On June 1, 1985, Air India's Chief Vigilance and Security Manager in Bombay sent a telex to Air India offices worldwide, warning of "…the likelihood of sabotage attempts being undertaken by Sikh extremists by placing time/delay devices etc. in the aircraft or registered baggage." The telex went on to set out specific security precautions to be implemented. These precautions included "explosive sniffers and bio-sensors [dogs]" as well as physical random checks of registered baggage, at least until June 30, 1985.

Air India forwarded the telex to the RCMP Officer in Charge at Pearson airport in Toronto, who sent it on to the Acting Officer in Charge in the RCMP HQ Airport

Policing Branch, requesting instructions on how to respond. The A/OIC sent a telex to CSIS, asking for an updated threat assessment in relation to Air India.

CSIS responded with a threat assessment indicating that it was unaware of any "specific threats" against Air India at the time.

In its submissions to the Honourable Bob Rae, the RCMP indicated that it had forwarded the June 1st Telex to CSIS along with its request for an updated threat assessment. The RCMP also told Rae that the heightened security measures it implemented included the use of explosives-sniffing dogs to check the passenger section of the aircraft prior to departure.

Both of these statements were incorrect.

The June 1st Telex not only was not sent to CSIS, it appears not to have been sent anywhere other than to HQ Airport Policing. It was not even sent to RCMP NCIB, the branch in charge of internal RCMP threat assessments.

The June 1st 1985 Telex was a key piece of the mosaic that never reached CSIS and was never integrated into the threat assessment process about Sikh extremism. The failure to forward the telex to CSIS eliminated any opportunity for CSIS to consider the information it contained about the threat of imminent attack in light of other information CSIS had received.

In his testimony, the former CSIS investigator in charge of the pre-bombing BC investigation into Sikh extremism stated that knowledge of the June 1st Telex would have given him a better understanding of the significance of the "loud noise" reported by CSIS surveillants when they followed Parmar, Reyat and an unknown person into the woods near Duncan on June 4, 1985. A Toronto CSIS investigator made precisely that connection shortly after the bombing when he zeroed in on the Duncan Blast surveillance report and identified the noise referred to as almost certainly being a test explosion rather than, as previously thought, a shotgun blast.

The November 1984 Plot is a similar instance of a pre-bombing failure to integrate important information into the mosaic of threats. In September 1984, the RCMP learned, through "Person 1," that Sikh extremists were organizing to bomb an Air India plane but failed to share this information with its own HQ, with CSIS or with other agencies. CSIS did not learn of the existence of this plot until late October 1984, when the Vancouver Police Department received essentially the same information from "Person 2", which it then shared with CSIS and with the RCMP. The RCMP, however, failed to inform CSIS that this information constituted corroboration of earlier information from another independent source, Person 1.

CSIS was aware of several threats against Air India during the month of October 1984 and, prior to learning of Person 2's information, issued a threat assessment

noting that an attack in Canada was remote but could not be ruled out. After receiving Person 2's information, CSIS updated its assessment to a "real possibility" that Sikhs would damage an Air India plane.

It was not until March 1986, when the RCMP performed a post-bombing file review, that Person 1's statement to police in September 1984 about a man in Duncan who could manufacture "nitro" for blowing up an Air India flight come to light. If CSIS had received this information in the pre-bombing period, the significance of the excursion by Parmar and Duncan resident Inderjit Singh Reyat into the woods near Duncan would have undoubtedly been assessed in a more sinister light.

This chain of events dramatically illustrates the role that corroborating information can have on the threat assessment process. It also highlights how a lack of all relevant information can result in a serious potential threat being disregarded.

Quite aside from the information provided by Bartleman and intelligence about the June 1st Telex and the November Plot, there were other key pieces of the mosaic in the possession of government agencies that CSIS never received and therefore couldn't use in its threat assessment.

After the close of the hearings, the Commission became aware of relevant information in the possession of the Communications Security Establishment. CSE information is subject to rigorous National Security Confidentiality requirements, and little detail can be revealed about this information except that the information indicated that specific security measures, substantially similar to those listed in the June 1st Telex, were to be undertaken inside and outside of India for Air India flights due to threats of sabotage and hijacking by Sikh extremists. Furthermore, Indian airports were undertaking security audits in response to the threats and the Government of India had shown an increased interest in the security of airports against the Sikh terrorist threat in the month of June 1985. This latter fact would have clearly called into question RCMP and Transport Canada officials' view that threats, such as the June 1st Telex, were provided by Air India solely as a means to obtain additional security for free. This additional information might, in itself, seem unremarkable, but in the context of the June 1st Telex, as well as other information known to agencies of the Canadian government in June 1985, it should have suggested a significant risk of a bomb attack on an Air India flight in June 1985.

There is no record of the CSE information being provided to CSIS.

The June 1st Telex and the CSE information were more than enough, had they been assembled in one place and assessed by a skilled analyst, to have mandated an upgrading of security and the implementation of responsive measures at Pearson and Mirabel airports and, arguably, at airports with connecting flights to Air India, so as to respond to a high threat of sabotage by bombs concealed

in checked baggage. The Commission accepts the expert evidence given at the Inquiry that, even on its own, the June 1st Telex clearly should have led to this upgrade in security.

Bartleman's evidence is not essential to arrive at the conclusion that the Government knew enough about the pre-bombing threat to make its failure to implement responsive security measures inexcusable. However, the prominence given to the testimony of Bartleman by the Government makes it necessary to conduct an evaluation of his evidence. With an understanding of what was known by the Government in the pre-bombing period, Bartleman's evidence can now be assessed in its proper context.

Despite the aggressive insistence of the Government to the contrary, there is nothing implausible about the existence and subsequent disappearance of a document referring to a threat directed against a Canadian Air India flight. It is possible that the passage of over two decades may have blurred some details in Bartleman's recollection, but the essence of his testimony is credible. The Commission, applying the elements of common law assessment of evidence, finds him a credible witness. He had nothing to gain from coming forward with his evidence and he was fully aware that his evidence would be vigorously attacked.

The Commission accepts the possibility that a document such as that described by Bartleman would have been ignored and then subsequently could have gone missing from the Government's documentary holdings because:

> The documentary holdings for the pre-bombing period are incomplete.
>
> DFAIT archives have been purged with no index of destroyed documents.
>
> CSIS, as a matter of policy, destroyed source documentation once it had been reviewed and any intelligence reports had been written.
>
> Despite statements made in documents before the Commission and in corroborating testimony at the hearings that asserts that in the pre-bombing period the RCMP was in receipt of a large volume of threats to Air India forwarded by Air India itself, the number of RCMP documents produced to the Commission falls well short of that description.
>
> The state of CSE documentary holdings from the pre-bombing period is unclear and the holdings themselves almost certainly incomplete.

Various government witnesses claimed that information about a threat against an Air India flight would have made an impression on them and that they would have raised an alarm immediately. This assertion, however, is inconsistent with what is known about the reaction to threat information received by the Government of Canada in the spring of 1985 for which documentary evidence remains. Such threat information, including the June 1st Telex, received little if any reaction.

A government witness who stated that he would have remembered and reacted to any bomb threat concerning Air India had to be reminded of the existence of an April 1985 threat against an inbound Air India flight. He defended his lack of response in that case on the basis that there were no security precautions necessary to deal with a threat against an inbound flight. Nevertheless, the failure to raise an alarm and the absence of documentary reference to this threat in any other material from the pre-bombing and post-bombing periods parallels what happened to the June 1st Telex.

A CSE witness who attempted to attack Bartleman's credibility asserted that he would have warned the Government of any threat against an Air India flight, as he had done months earlier when he saw a reference to the November Plot. He apparently was unaware, however, of the existence of the CSE information about security measures being mandated for Air India operations, inside and outside of India in response to threats of sabotage by Sikh extremists and information that Indian airports were conducting security audits in light of these threats. This is information whose relevance to the Air India bombings the Government disputes to this day. The very fact that the relevance of the CSE documents is disputed is illustrative. If past and current CSE officials cannot, even in hindsight, make the connection between this information and the threat to Flight 182, it should hardly be surprising that its relevance was unappreciated in 1985.

It remains unknown how accurate the threat information seen by Bartleman may have been. As he freely admitted, the information he saw merely suggested the existence of a threat and he had no way to assess its seriousness or credibility. The RCMP witness who testified that the Force received threats to Air India before every flight used that fact as justification for the RCMP's view of these threats as "floaters" – sent by Air India in the hopes that the Canadian Government would provide additional security without additional cost. This account of the RCMP's view of the credibility of threats to Air India issued at the time is consistent with Bartleman's account of the dismissive and even hostile reception he received when he sought to bring the information to the attention of the Force. It is also consistent with notations in earlier documentation about a seeming annoyance on the part of the RCMP with being "second-guessed" on security decisions by a member of External Affairs.

Even if Bartleman saw nothing more than what was contained in the CSE information unearthed by the Commission, it is likely that it would have been enough, given his knowledge of Sikh extremism in Canada, to convince him that the threat needed follow-up. The fact that Canada had the largest Sikh diaspora

in the world, that June was a time when there was a very high risk that some action would be carried out against Government of India interests and that Air India was a possible symbolic target, all would lead anyone with his knowledge and experience in the area to raise questions about what precautions had been taken. This was precisely what Bartleman did.

3.4 Response to the Threat

Prior to the bombing, the Government as a whole had the following information relevant to the risk that Sikh extremists could successfully carry out the bombing of an Air India plane:

> It was aware that Sikh extremists were serious about a terrorist attack during June 1985 against a symbol of the Government of India. It knew the identity of the extremists likely to be involved in such an attack.
>
> It was aware that Air India's flights were likely to be a target of Sikh extremists and that a likely means for such a terrorist attack was a time-delayed explosive concealed in checked baggage.
>
> It was aware that the most serious threat to civil aviation was no longer hijacking, but sabotage.
>
> It knew that Transport Canada's regulatory regime was inadequate to deal with this sort of threat and that the specific security measures currently instituted by Air India were inadequate and were based on unreliable technology and untrained screeners.
>
> It was aware of rules and procedures that could have been prescribed by Regulation, and that would have been more effective in responding to security risks posed by interlined baggage and by baggage checked-in by passengers who did not show up for their flights.
>
> It was also aware of more effective procedures, such as passenger-baggage reconciliation, and practices for screening baggage and identifying potential risks.

Nevertheless, because the Government did not address what was, by its own evaluation, a security regime wholly inadequate to identify and respond to known serious threats, it failed to prevent the bombing of Air India Flight 182.

3.5 The Bombing of Air India Flight 182: A Litany of Security Breaches

By June 1985, the threat of terrorists attempting to exploit vulnerabilities in the aviation security system by placing explosives in checked baggage had been well understood by Transport Canada for at least five years. The concern about the threat of sabotage was so great that in 1980, Canadian aircraft operators and manufacturers had requested that Transport Canada develop screening techniques and equipment for detecting explosives. Even so, as of June 22, 1985, the standard security procedures in place at Canadian airports were still oriented towards the prevention of hijacking. These measures were focused upon preventing potential hijackers from carrying weapons aboard an aircraft and there existed no screening requirement for checked baggage.

CP Air in Vancouver was operating at a "normal" threat level on June 22, 1985, despite the fact that Transport Canada and elements of the RCMP possessed voluminous information about the high threat to Air India and despite the fact that Transport Canada was aware that CP Air had flights connecting with Air India. "M. Singh" became disruptive and insisted that his luggage be tagged through to his final destination in India, ostensibly to save him from having to pick them up and check them in again when the CP Air flight arrived in Toronto. The CP Air agent violated CP Air's own security protocol by tagging the luggage through to Air India 181/182 even though the passenger did not have a confirmed seat aboard these flights. CP Air also took no steps to remove the bag checked by "M. Singh" when he did not board the aircraft. Upon arrival in Toronto, this "unauthorized" bag was placed on board Air India Flight 181 by ground staff at Pearson Airport. Due to its own deficient protocols, Air India was unaware that this bag had been loaded.

Meanwhile, earlier that same day at Pearson Airport, Brian Simpson, an Air Canada summer employee at the time and now a lawyer, was curious about the very large *Kanishka* aircraft stationed outside the international departures area. Although he was not authorized to be inside the aircraft, he was able to walk to, and board, the plane; explore its interior for approximately 10 minutes and leave without being challenged by security officials or other airport staff. Simpson, who had observed numerous lapses in security in his time working at Pearson, was not surprised by this inattentiveness. He testified that, at the time, security doors that were meant to be locked were frequently kept open, and that doors secured by coded locks often had the access codes written on the wall nearby.

In that same period, similar lax security procedures had been observed at Vancouver and Montreal airports. Transport Canada was aware of the lax security culture prior to the bombing. Although annual security surveys were not conducted at Mirabel, they had been at Pearson in 1983, 1984 and in the spring of 1985 and at Vancouver airport in 1982 and 1985. A 1982 Transport Canada report noted that many aspects of Canada's security program were cosmetic

and incapable of resisting a well-organized terrorist attack. Nevertheless, this situation was permitted to persist.

While RCMP HQ had assigned a level of security for the Air India flights in June that called for an RCMP explosives detection dog (EDD) team to search the passenger section of the aircraft, as well as any suspect luggage, prior to departure, the EDD teams were unaware of the state of alert at the time. On June 22, 1985, the EDD teams were all in Vancouver for training, leaving the Toronto airport without any trained dogs, and with only the RCMP Hand Search Team as backup. In case of a security alert, the role of the Hand Search Team (despite its name) was merely to search the interior of the aircraft and to oversee a process of passenger-baggage matching.

Although Montreal's Mirabel Airport had arranged for access to the Sureté de Québec dog team if necessary, this team was not at the airport prior to the flight's departure, and despite the identification of three suspicious bags that were not loaded, neither the passenger section of the aircraft nor the flight's checked baggage was searched.

Due to the constant high threat to Air India operations, Air India's security program called for the use of X-ray machines at both Pearson and Mirabel to examine checked baggage for explosives before any bags would be loaded aboard their aircraft. Air India also employed an electronic explosives detection device, the PD4, as a back-up when the X-ray was broken or not available. The PD4 device had been tested and proven totally ineffective by a member of the RCMP at Pearson in early 1985, in front of a group of representatives from Air India, Transport Canada, Peel Police and the RCMP. At the time, the RCMP told Air India that it had no confidence in the efficacy of the PD4 sniffer device. However, it did not intervene to prevent its use as part of Air India's security plan for flights in early 1985, prior to the arrival and installation of its X-ray machine, or thereafter, as a back-up to the X-ray. When Air India's X-ray machine at Pearson airport, which had malfunctioned at least once before in June 1985, and which had experienced reliability problems in the past due to mistreatment, broke down after scanning about 50-75 per cent of the luggage on June 22, 1985, the Air India security officer decided that the remaining bags would be examined for explosives with the PD4 sniffer device instead. Despite the high threat level assigned to Air India flights, neither Burns Security nor Air India informed the RCMP about the X-ray equipment breakdown on that day, and RCMP members did not monitor or even liaise with Air India or the screeners in the nearly 5 hours between the time the machine broke down and the time the plane departed.

The Burns Security employees, private security officers employed by Air India to conduct checked baggage screening, had no prior experience or formal training in the operation of the PD4. There was no supervision by Canadian government officials. Burns employees were not instructed about how to interpret the sounds the PD4 made, and no one informed the Burns supervisor or the Air India Security Officer that the device may have reacted to some of the bags it scanned. Then, without further contemplation of the potential danger they posed, the bags were loaded onto the aircraft.

Sometime before the check-in screenings at Mirabel were completed, Daniel Lalonde, now an Ontario Provincial Police officer, who in 1985 worked for Burns Security, was asked to leave his post at a security checkpoint to assist a number of other security officers in the X-ray scanning of checked baggage. Lalonde had never operated, nor even seen, the type of X-ray machine that was in the baggage room. The extent of his training to examine carry-on baggage with an X-ray machine was a one-hour video showing images of a handgun and a stick of dynamite as the types of dangerous articles he was to watch for, and on-the-job learning. In the course of screening the checked bags, he and the other Burns employees identified three bags whose contents appeared suspicious. The suspicious bags were placed on the floor next to the X-ray machine. The Burns supervisor notified an Air India representative about the bags, but the RCMP was not alerted until about 2 to 3 hours later. When RCMP officers arrived at the baggage area, they found that the suspect bags had been left unattended on the floor.

The Air India security officer had arrived from Toronto about 2 hours after the suspect bags were discovered and decided that they should not be loaded aboard the aircraft. Lalonde overheard the Air India security officer mention his concerns about the cost of delayed takeoff when he made the decision to clear Air India Flight 182 – which was running behind schedule - for takeoff. In 1985, the cost of delaying the takeoff of a wide-bodied jumbo jet like the *Kanishka* was between $10,000.00 and $18,000.00 an hour.

When the SQ dog handler was called in by the RCMP on the night of June 22, 1985, he believed he was being called to search the plane and its checked luggage. However, the aircraft had already departed prior to his arrival and he was only able to search the three bags that had been left behind.

On June 23, 1985, at 07:14 GMT, Air India Flight 182 disappeared from radar screens.

It has often been said that the failures that ultimately permitted the loading of the bomb onto Air India Flight 182 on June 22, 1985, were the result of a series of tragic coincidences and overlapping lapses. While this is true in some respects, the many deficiencies and errors that were observed on June 22, 1985, were also the predictable outcomes of poor regulatory and funding decisions and of a lack of leadership, which combined to create an environment ripe for exploitation by would-be terrorists. Air India's operations in Canada were known to be a "soft target" and little stress on that system was required to set off the chain of failures that ultimately led to disaster.

History has demonstrated the tragic extent of harm that can result from an ineffective aviation security regime. The risk to aviation security demands that there be a well-coordinated system of multiple, overlapping layers of security measures and a pro-active and responsive regulatory regime that is consistently reviewed for its effectiveness, in the context of past, present and future threats. This was not the type of security regime in place at Canadian airports in 1985.

3.6 Resources and Privatization

The 1980s was a period of deregulation, downsizing, and privatization.

Though the *Aeronautics Act*, the primary regime setting out authority for the regulation of civil aviation in Canada, gave the overall responsibility and authority to the Minister of Transport to "supervise all matters connected with aeronautics," the regulatory regime in place put much of the responsibility for aviation security onto private actors. In this context, privatization could only work if the Government discharged its duty to take reasonable steps to protect its citizens through active monitoring and oversight of security operations. Profit-conscious carriers might be tempted to save money by reducing security expenditures, so it was reasonable to expect an increased level of Government intervention when it was aware of a heightened threat.

In the pre-bombing period, however, Government resources for airport security were scarce and thinly stretched. Transport Canada faced major budgetary constraints as the incidence of hijacking attempts and other criminal acts against civil aviation declined, and it became increasingly difficult to justify the costs of security expenditures. Transport Canada airport managers were under continuing pressure to reduce spending, which resulted in local constraints being applied to their budgets. This had an impact on RCMP airport policing resources which were negotiated locally with Transport officials at the airport level.

In 1985, the RCMP was mandated by contract with Transport Canada to perform specific police and security duties at designated airports, including: formulating, disseminating and auditing airport emergency procedures; collecting, evaluating and disseminating intelligence; and guarding against sabotage of airlines and the airport. The RCMP Airport Policing program had experienced progressive budgetary cutbacks for years. By 1983, the cutbacks had reached a level that made it impossible to meet its obligations to respond to threats to airlines in some locations. By June 1985, the RCMP's presence had been downsized at most airports to include traffic control, a uniformed presence within and outside the airport and the occasional patrol of the perimeter.

Transport Canada inspectors were directed to monitor airports and to alert the carriers to any shortcomings in their security systems. There were, however, only 11 inspectors across Canada to conduct such reviews for the roughly 70 carriers operating across the country. By June 1985, inspectors had not completed more than 10 per cent of their workload for that year in any region, and in some regions no aviation security inspections had yet been conducted.

Entrusting vital security responsibility to the carriers themselves, in combination with the lax security culture at airports and the lack of resources for Government oversight and training, was a recipe for disaster. Without continual and thorough monitoring of the air carriers, airport personnel, and security staff within that system, carelessness and complacency flourished.

Both foreign and domestic air carriers were required to establish, maintain and carry out certain security measures at airports, including passenger and baggage screening. Private security officers were contracted by the air carriers to staff the security checkpoints and to conduct pre-board screening of passengers and luggage. In 1985, the *Aeronautics Act* limited the designation of "security officers" to properly qualified personnel. Security officers were required to complete Transport Canada's passenger inspection training program with an average mark of 70 per cent and refresher training was also required within 12 months of any previous training. However security service contracts tended to be awarded by airlines to the lowest bidder. The security officers were paid minimum wage, and were unqualified to do their jobs, as many had either never taken the mandatory Transport Canada passenger inspection program or the required refresher training. Transport Canada was aware of these deficiencies but took no action to remedy them.

While Transport Canada required its own employees to undergo background and criminal record checks in order to obtain security clearance, the employees of the carriers working at airports across Canada were not subject to either criminal record checks or credit checks. They nevertheless had access to airport restricted areas and aircraft. Following the bombing, CSIS checked the names of the janitorial staff with access to the location where the bags containing the bombs were placed on the aircraft at Vancouver International Airport. CSIS found that multiple individuals among the airport janitorial staff, who had wide access to the airport and could move about virtually unnoticed, had connections to extremist Sikh organizations. The brother of Ajaib Singh Bagri, the latter of whom was suspected of a role in the Air India bombing, was among them.

Security companies were generally under the direct supervision of an air carrier's customer service section, whose focus on keeping passengers happy by minimizing delays and inconvenience often conflicted with security priorities. Contracted screening companies were often urged to rush through screening as quickly as possible. Prior to the bombing, in March 1985, Air India's acting airport manager for Mirabel and Pearson airports expressed concern about the numerous complaints that were being received about the delays of its flights leaving Toronto. Air India headquarters had set a "2 hours ground time" limit for delayed flights that was to be "strictly followed." Simply put, customer service and other commercial concerns trumped aviation security.

In combination with the lack of resources for oversight, the privatization of airport security also led to a "hands off" approach towards oversight at Transport Canada. Transport Canada was aware of the potential value of passenger-baggage reconciliation and considered it an effective security measure for high threat situations. Confirming that all checked bags were matched with travelling passengers required additional time before a flight could depart and caused inconvenience to passengers.

Prior to the bombing, Transport Canada was tentatively considering a requirement for X-ray inspections as a viable alternative to the lengthy

passenger-baggage reconciliation process. Transport Canada appeared to view X-ray technology as something of a panacea, despite the poor resolution of the X-ray images and the high degree of skill required to appropriately interpret them.

Concerns about costs and delays influenced Air India's decision to use technological solutions to speed up security screening wherever possible. In 1985, Air India's security plan for operations in Canada included screening all passengers and their carry-on baggage by use of X-ray scanners and walk-through metal detectors as well as X-raying or using the PD4 explosives detection device on all checked baggage as a standard measure prior to its being loaded aboard aircraft. This plan was "informally" approved by Transport Canada with some minor modification. However, in spite of its international obligations to approve, monitor and comment upon air carrier security plans, monitoring was effectively non-existent.

Burns employees received practically no formal training in the examination of baggage with an X-ray machine. The utility of any screening technology necessarily depends on the skill of those employed to use it. Air India's X-ray machine was poorly handled and poorly maintained, had malfunctioned on several occasions, and ultimately broke down on the eve of the bombing. Given the state of X-ray technology at the time, the efficacy of the machine in detecting explosives was already quite limited, and these other factors further compromised its usefulness. Despite the high threat situation, the Government raised no objection to Air India's continued use of this machine or to the use of the proven-ineffective PD4 as a replacement.

The first Air India flight from Pearson took place on January 19, 1985. At that point, Air India's checked baggage X-ray had not yet been installed, and so the PD4 was used instead to examine the checked baggage destined for the flight, despite the advice from the RCMP not to rely on the device. The RCMP and Transport Canada did nothing to intervene, in spite of a second failed test conducted by the RCMP that day, and in spite of the fact that both agencies had been evaluating the progress of explosives detection technology through the late 1970s and early 1980s, and had been finding that such devices were generally unreliable. In light of the primitive state of explosives detection technology at that time, Air India's reliance on the PD4 was alarming.

The Government retained ultimate authority at the airport to decide whether or not to allow a flight to depart, and could detain a plane or take other action to ensure a flight would not depart in dangerous circumstances. In reality, however, the combination of the Government's laissez-faire approach and its lack of oversight ensured that, aside from obvious circumstances of inclement weather, the Government would almost never have the information nor the will required to exercise this power.

3.7 Lack of Sensitivity to Emerging Threats

In a dynamic environment in which new threats can emerge at any time, an effective aviation security regime requires a high degree of flexibility in order to identify emerging threats and then to tailor a coordinated response, sensitive to the relevant risk. Risk assessment requires a calibration of the vulnerabilities that make a system more susceptible to attack or exploitation by terrorists, and of the potential for harm in the context of a particular threat. In 1985, numerous discrete deficiencies aligned to create a situation in which Canada's state of aviation security was utterly unable to identify and respond to emerging threats.

3.7.1 Information Sharing and Coordination

The involvement of multiple actors in the protection of civil aviation – including Transport Canada, the RCMP, Air India and Burns Security – meant that a high level of coordination was required to ensure that those responsible for implementing security measures were aware of relevant threats and understood their responsibilities in terms of responding to any given threat. In 1985, each actor operated in its own silo, without an understanding of how any piece of information it obtained related to the broader picture of aviation security. Even within each agency, there was significant uncertainty about how information was to be shared internally and about how measures were to be implemented in response to it.

As stated earlier, the RCMP did not share the June 1st Telex with either CSIS or Transport Canada, which could have then taken steps to impose additional safety measures. Over two years later, in October 1987, a member of Transport Canada's HQ Civil Aviation Security Branch first learned of the existence of the June 1st Telex, and was alarmed by the many questions it raised as well as by the failure of both the RCMP and Air India to take proper action.

Transport Canada's ability to disseminate threat intelligence to airports was impeded by a lack of its own secure national communication system. Instead, it had to rely on the RCMP to transmit classified intelligence to personnel at airports. Multiple steps involved in sending intelligence reports in an emergency created a clumsy protocol and, as a result, major airports did not always receive classified security intelligence quickly, if at all. Transport Canada officials found that, even where an RCMP airport detachment received classified information well in advance of Transport Canada officials, the RCMP was often reluctant to pass such information on.

The lack of understanding of the phenomenon of Sikh extremism, and the failure to appreciate the symbolic significance of the Indian Government's ownership of Air India, complicated the situation further. As a result, when CSIS issued threat assessments indicating that the threat to Indian property and personnel was high, the relevance to Air India wasn't understood, and therefore, these warnings were not taken into account and shared with those charged with making decisions about the protection of Air India.

Excessive secrecy further compromised the ability to respond effectively to threats. The "need-to-know" principle prevented information from reaching the critical decision-makers on the front lines. In June 1985, when the RCMP received classified intelligence indicating that an incident was imminent, it took the position that this information could not be shared with Transport Canada officials. Without this information, it was impossible for Transport Canada to make its own assessment regarding the imposition of additional security measures and whether funding should be released to the RCMP for the extra manpower to respond to the threat.

Frontline workers such as Air India personnel and Burns Security agents were similarly deprived of information specifying what they should be alert for. The greater detail that security officers have about the nature of the threat, the better they will be able to direct their energy and tailor their response in a meaningful way. Providing detailed threat information to frontline workers would have been the optimal strategy.

With airports on a generalized "high threat" alert over long periods of time, even as security incidents in day-to-day work were extremely rare, threat fatigue as well as a lax security culture further eroded vigilance among airport workers.

Confusion regarding which organization held the ultimate responsibility for decision-making in a given threat situation further hindered responses. Some RCMP officials believed it was their responsibility to determine the threat level and the appropriate response; Transport Canada airport officials disagreed with this assertion. Confusion over responsibility led to acrimonious personal relationships between officials from Transport Canada and the RCMP Airport Policing detachment at Pearson.

Transport Canada had its own policies and protocols, and had the ability to impose additional security measures at the airport if warranted by the level of threat, but was not kept informed of the level of security the RCMP was applying at the airports or of the protocols the RCMP followed. The lack of coordination and understanding of other agencies' protocols increased the risk of disagreements between them, and inflated the potential for security gaps to arise.

RCMP Airport Policing did not regularly inform others, including the individuals expected to implement security measures, of the security levels it was implementing in response to current threat information. The RCMP dog handler for Pearson was unaware that the Air India flights in June were operating under an increased level of security which required his presence, and that of his dog, at the airport to search the passenger section of the aircraft prior to departure and to check any suspicious luggage. Despite the heightened security level, RCMP dogs across Canada were on training that weekend. As a result, on June 22, 1985, Canada's busiest airport was left without the security services of an explosives detection dog.

Even though the same weekly Air India flight stopped at Pearson and Mirabel, there was so little coordination between RCMP airport detachments that, despite threats preceding almost every Air India flight, throughout most of the first half of 1985, Air India was afforded different levels of security at each airport. While at Mirabel airport, Air India was given the second highest level of security, at the Pearson detachment, the same flight was provided only the minimum possible level of security. On May 31, 1985, External Affairs noticed this discrepancy and intervened to request that the level of security for Air India in Toronto be made consistent with that provided in Mirabel.

3.7.2 Lack of Risk Analysis and Misuse of "Specific Threat" Concept

In the aviation security context, a bomb threat that was assessed to be a "specific threat" would trigger an elaborate airport emergency protocol that involved the offloading of all luggage from an airplane, a search of the plane, passenger-baggage matching and the use of an explosives-sniffing dog to search all luggage. Had this protocol been employed on June 22, 1985, the bomb that ultimately brought down Flight 182 almost certainly would have been identified, but, on the eve of the bombing, the Government of Canada did not implement these or other search methods to identify bomb-laden luggage.

Given the numerous pieces of threat information received by the Government of Canada in the pre-bombing period, including warnings that specified the use of time-delay devices in registered luggage checked onto an Air India flight, the obvious question is: why did the Government not take appropriate, timely, responsive, and protective action?

The significance of a "specific threat" in the 1985 threat-response regime was limited to the circumstance of an emergency phone-in bomb threat. The definition of "specific threat" used by Transport Canada officials required details about the precise date, time, and even flight number. Importantly, the "specific" versus "non-specific" characterization, according to this definition, was to be made in time-sensitive circumstances, solely on the face of a particular threat without the need for additional or corroborative information. This narrow "specific threat" definition in use at the airport was never meant to apply outside of the emergency context.

In practice, the concept of specificity was inappropriately used. The quest for a "specific threat" impeded the proper analysis and response to threats. The "specific threat" concept was misapplied to threats received outside of the emergency context and was used in an all-or-nothing manner, often to deny additional security.

The "specific threat" concept had no relevance to the security that should have been implemented in relation to Air India Flight 182. The Government of Canada received many threats, including the June 1st Telex, well in advance of the flight. In these circumstances, there was sufficient time for an intelligence assessment, which could then have been relied on by officials to tailor an

appropriate response to the threat. Indeed, the RCMP had developed separate non-emergency security protocols to be implemented in response to CSIS's assessment of the threat. Misapplying Transport Canada's highly restrictive emergency definition, which was designed for a time-sensitive phone-in threat, to threats received outside of an emergency context, ensured that essentially no threat received by other means would ever be viewed as a "specific threat."

Despite the Government's awareness of the paradigm shift in aviation terrorism from hijacking to sabotage, its threat-response protocols remained targeted to the prevention of hijacking. The Government's continued focus on the concept of "specific threat" serves to distract from the real issue, which is that the applicable protocols in 1985 were not responsive to the risk of sabotage and were thus woefully inadequate in the circumstances.

When airport policing obtained a threat assessment from CSIS, the level of threat identified by CSIS was then used by the RCMP to determine the type of deployment with which to respond. A "security grid" set out five levels of security and the type of deployment to be effected at each level. A "high" threat, for example, would elicit a "level 4" response on the security grid, whereas "level 5" was reserved for a so-called "specific threat." To add to the confusion, in CSIS's lexicon, for a threat to be "specific" required not only a high degree of specificity, but also a degree of corroboration.

Whether the threat was "specific" or not, the actual difference in deployment between levels 4 and 5 was nearly insignificant, amounting to the use of an additional airline vehicle stationed airside, and another that would follow an RCMP patrol car while the escort of the aircraft was underway. Even at the highest level of security, the measures would have done nothing to prevent the loading of a time/delay device in registered luggage.

In mechanically translating threat levels into security deployment without even considering whether the measures dictated by the grid were at all responsive to the nature of the actual threat, the RCMP failed to appreciate the inherent need for risk analysis in order to appropriately translate threat information into operational deployment. This lack of understanding or appreciation for risk led to absurd situations.

The RCMP implemented additional security at Pearson airport in light of threat information received in late May 1985. However, due to an oversight, Transport Canada had not budgeted for overtime for that year. This increased level of security was maintained throughout June, but without Transport Canada's consent, additional funds would not be released to pay for the additional manpower. A dispute erupted at Pearson airport in June 1985 between Transport Canada and RCMP officials over the payment for this additional RCMP security. When additional, "highly classified," threat information was received by the RCMP in early June that left RCMP officials at Pearson with no doubt that "something was going to happen," the seriousness of this undisclosed threat was argued as an abstract concept and was used to justify payment for the security

already in place. There was never a consideration of whether or not the existing security was an appropriate response to this new threat. In fact, no adjustment to the existing security was made in light of this information. Similarly, when the June 1st Telex was received at Pearson, RCMP Airport Policing simply maintained the existing (non-responsive) "level 4" security already in place, given that CSIS (which was not provided with the Telex) was unaware of any "specific threats."

In the context of this Inquiry, the Government continued to misuse the concept of "specific threat" in support of its argument that the June 1st Telex was not specific, thereby implying that additional security was not warranted. Dr. Leiss, an expert in the area of risk communication and risk management was shown the June 1st Telex and was astounded by its specificity. He stated that in the area of aviation security it would be extremely rare to get such a precise piece of information. In light of the high risk situation at the time, the June 1st Telex should have stood out and officials would have been justified in "basically pulling out the stops."

In fact, the reason for the inadequate response to the June 1st Telex was not because it lacked specificity. The telex was sufficiently specific that, had anyone considered doing so, a sensitive response would not have been difficult to implement. Air India was operating only one flight out of Canada each week; the telex specified a narrow time period and suggested measures that would be responsive to the nature of the threat. Deficient protocols and a lack of understanding of the purpose of what it was doing resulted in the RCMP's failure to understand the significance of the June 1st Telex and in its ineffective response as a consequence.

3.8 Ineffective Regulation

In addition to the requirement that the system have the flexibility to quickly identify and respond to individual threats, regular assessment of whether the legislative and policy framework was adequate to meet the nature of potential threats was essential. By 1985, such assessments had been undertaken and serious problems were thereby identified, but nothing was done to rectify them.

While Transport Canada had long been aware of the threat of sabotage as well as of the many weaknesses in its airport security, the ability to correct these weaknesses was hampered by deficiencies in its regulations. The problematic nature of the regulations was well understood prior to the bombing, yet the Government delayed bringing the *Aeronautics Act* and the accompanying security regulations up to date and to a level capable of meeting the threat of terrorism.

Perhaps surprisingly, regulations relating to observation, inspection, and searches of passengers, baggage, and cargo were already authorized under the existing *Act*. Draft regulations, most of which could have been passed under the *Aeronautics Act* then in force, and which could have remedied many of

the identified security problems, had been circulating since 1982. However, Transport Canada sat on them, preferring to await passage of a bill that was before Parliament at the time of the bombing and that would have significantly amended the Act and given the Minister of Transport broader powers to regulate with respect to aviation security. Though some officials recognized that the draft regulations were urgently needed, nothing was put into place until after the bombing.

Transport Canada generally took the position that as long as an airline's security plan met the basic and vague requirements outlined in the regulations, it was valid. In the words of one official, the regulations provided that a valid "security plan" required only that there be a "system" in place – whether that system was "good, bad, or indifferent." But even without the planned amendments to the Act, it would have been possible to update the regulations to require that air carriers provide specific details in their security plans. Such details could have included the designated security officers assigned to provide services for the air carrier, and a description of their required training, as well as the procedures and guidelines to be used by the carrier for screening persons, personal belongings, carry-on baggage, checked baggage and cargo. Regulations under the authority of the existing legislation could also have authorized the Minister of Transport to independently request changes to air carrier security plans where such changes were deemed necessary for civil aviation security.

Regulations under the then current Act also could have addressed numerous other deficiencies that had been recognized before the bombing. Regarding the threat of sabotage, regulations could have been passed to direct that air carriers take steps to prevent the carriage of explosives in checked baggage. Additional security measures to be implemented during a high threat situation, at a minimum, could have included matching all checked baggage to the passenger manifest prior to departure, X-raying or providing a manual search of all baggage using an explosive detection device or dog and handler or delaying the transportation of baggage on high-risk flights for a specified period of time.

Regulations could also have provided for more consistent and effective responses to the security risks posed by "unauthorized, infiltrated" baggage by requiring that checked baggage only be accepted from validly ticketed passengers and that all checked bags be personally identified by their owners. The level of training of airport workers could have been addressed by regulations stipulating that no personnel would be allowed to perform passenger, ticket, and baggage-related duties unless they had completed approved security training courses.

In light of the frequent security breaches that plagued many airports, a number of other remedial security provisions were also possible. Airport operators could have been required to keep records of all keys in their possession, to record the names of the individuals who were issued airport keys, and to prohibit anyone from entering or remaining in a restricted area without possessing and visibly displaying their identification card unless otherwise authorized.

All of these regulations would have been possible under the *Aeronautics Act* in the pre-bombing period. In fact, most were already contained in the 1982 draft regulations and could have been passed long before the bombing, but for Transport Canada's inaction.

What the *Aeronautics Act* in the pre-bombing period did not provide was sufficient authority to make regulations dealing with enforcement. One of the main deficiencies, identified long before the bombing, was that if an inspection of an air carrier uncovered a security issue, there was no authority for enforcement action other than either a written reprimand or a total revocation the airline's landing rights at Canadian airports. There was nothing in between. There was no specified penalty for the failure of an air carrier to follow the requirements of its own security program. This was a fact that was highlighted when, after the bombing, Transport Canada concluded that no enforcement action could be taken against CP Air for interlining the "M. Singh" bag directly to Air India Flight 181/182 without the passenger having a confirmed seat.

While technically it was an offence to breach the regulations, the possible fines against carriers were not meaningful. Only after the bombing was the Act amended to authorize large fines (up to $25,000) against corporations upon conviction of a breach of the Act, regulations, or orders.

Post-Bombing: RCMP/CSIS Cooperation

3.9 Human Sources: Approach to Sources and Witness Protection

3.9.1 A Lack of Effective Governance

Without a central informed decision-maker to direct the entire Canadian counter-terrorism landscape, CSIS and the RCMP were left to proceed according to their own lights and based on their view of the needs and best interests of their own institution. In the competition and mistrust that ensued there were no winners.

The Air India narrative is littered with lost opportunities where the value of potentially useful information was nullified in the fallout of the agencies' self-interested actions. Nowhere was this more apparent than in the approach of the agencies to human sources and in their competition for access and control in connection with these "assets." In the end, few positive results were achieved, while the relationship between CSIS and the RCMP continued to deteriorate and sour.

CSIS reserved for itself the decision about when and how it would turn over criminal information to the RCMP. At times, it delayed turning over information, with the goal of squeezing as much information out of a source as possible before relinquishing control, often without keeping the records necessary to allow for the eventual evidentiary use of that source's information. When Mr. Z disclosed to CSIS the identity of the two Sikhs who he had been told were responsible for checking in the luggage, CSIS made a decision to hold off on

passing this information to the RCMP so that its avenues of investigation were not "jeopardized." CSIS ended up disclosing the information to the RCMP after about a month, but only because it learned that the RCMP was going to start a program of interviews that would turn up CSIS initiatives involving Mr. Z.

When CSIS investigator William Dean ("Willie") Laurie met with Ms. E in 1987, she told him that the night before Air India Flight 182 crashed, Ajaib Singh Bagri had come to her door, asking to borrow her car to go to the airport and telling her that only the luggage would be travelling. CSIS made a conscious decision to hold off passing this astonishing statement on to the RCMP, despite its clear and potentially transformative relevance to the criminal investigation, based on the dubious rationalization that Ms. E's information was mainly "historical" and incapable of being corroborated. In fact, the CSIS decision was motivated by a belief that the RCMP would bungle the approach to Ms. E and the result would be to end any hope of obtaining any further information from her. CSIS did eventually give the RCMP, verbally, enough information to discharge what it saw as its legal obligation, but did little if anything to ensure that the RCMP would be able to put together enough details to actually find her.

For its part, the RCMP appeared to live down to CSIS expectations and only began to pursue the Ms. E connection in 1990. Faced with RCMP allegations that it had withheld information about Ms. E in 1987, CSIS scrambled to uncover documentary corroboration that it had turned over the information. Though it failed to surface any such proof, CSIS nevertheless drafted a letter to the RCMP that provided assurances that all details had indeed been passed-on verbally, relying on cryptic internal RCMP telexes as justification.

The revelation that CSIS had withheld or delayed the passing of important criminal information only further fuelled the mistrust the RCMP had for CSIS and led it to feel justified in constantly questioning whether it had received all relevant information in relation to a source.

The case of Mr. A was equally unedifying. CSIS and the RCMP became aware of Mr. A at around the same time and both believed that he likely had key information about the Air India terrorist attack. The agencies met and agreed that CSIS would interview him first and would report the results of the interview to the RCMP. However, upon meeting with Mr. A, CSIS investigators realized that he was an extremely valuable source and that he had concerns about his safety that made him reluctant to share the details of his story. Despite the earlier agreement and the potential criminal relevance of his information, CSIS proceeded to provide Mr. A with assurances of confidentiality and turned him into a CSIS source. The information he had provided about Air India was subsequently provided to the RCMP, but without revealing that Mr. A was the source, relying for justification on the promise of confidentiality it should arguably never have made in the first place. Meanwhile, CSIS had no apparent problem in directly breaching its numerous assurances of confidentiality to Ms. E when it revealed her identity to the RCMP in 1990, once it became concerned about being blamed for not passing her information in the past.

Sources have rightfully been described as CSIS's lifeblood. CSIS's long-term investigation into Sikh extremism in the late 80's and early 90's depended on its ability to develop long-term relationships with individuals who could provide the Service with insight into what was happening in the Sikh community. Time and again, when CSIS did pass criminal information it received from a source to the RCMP, it ended up being forced to terminate its relationship with that source entirely. This was usually in order to protect the evidentiary value of the source's potential testimony from "contamination" and from allegations of "coaching" by CSIS, though at times it was simply the result of the source's refusal to cooperate further with anyone because of the RCMP's heavy-handed approach. The RCMP's concerns about the impact of CSIS involvement on eventual prosecutions were not unfounded, especially in light of CSIS's constant failure to preserve records of its dealings with its sources. On the other hand, the RCMP's bull-headed approach burned bridges for both agencies to the sources. The repeated loss of some of its most promising sources had, not surprisingly, a significant negative impact on morale among the CSIS investigators. CSIS's reluctance to pass information with potential criminal relevance over to the RCMP can accordingly be understood, if not condoned.

The combination of the RCMP's aggressive approach and its tendency to quickly discount sources often led to a lose/lose outcome: CSIS lost its source and the RCMP failed to gain any "evidence", or even any information, from the source. CSIS was ordered to hand Mr. A over to the RCMP as the result of RCMP lobbying for exclusive access. The RCMP dismissed Mr. A's utility after a 15 minute interview and left him fearing for his safety as a result of its unwelcome approach. Neither agency derived any benefit from the information he had to offer.

The result in connection with Ms. E was equally unsatisfactory. When the RCMP decided to approach Ms. E in 1990, CSIS Investigator Laurie warned that she would not be receptive to the police. The RCMP charged ahead regardless, with its usual aggressive approach. Laurie, the person with whom she had the best rapport, and who by then had transferred back to the RCMP, was excluded from the process as soon as possible and not re-involved until 1997. Ms. E was subjected to a long audio-taped interview at RCMP headquarters, during which she expressed considerable fear and reluctance. She was repeatedly approached by an ever-shifting cast of RCMP investigators who showed little concern for her feelings or her privacy. Ultimately Ms. E refused to cooperate with police any further and feigned memory loss when she was called to testify at trial.

It was not only the RCMP's aggressive approach to sources that caused CSIS concern. CSIS saw the RCMP place potential sources and witnesses in jeopardy by failing to implement adequate measures to protect them or to ensure that the confidentiality of their information was maintained. CSIS was shocked by the RCMP's failure to seal its Information to Obtain and thus to protect Ms. D's identity. It was similarly dismayed to learn about the RCMP's persistent aggressive approaches to Ms. E, often in public places or within earshot of others, which clearly placed her at risk. At times, even members within the RCMP took issue with the Force's handling of sensitive information. RCMP NCIS

Surrey investigators expressed concern that RCMP HQ had widely distributed correspondence within the RCMP that could identify Tara Singh Hayer as the source of information about an alleged confession by Bagri about delivering the bag to the Vancouver International Airport on the eve of the bombing.

The squabbling over sources was unremitting. CSIS complained of not being informed about RCMP plans to send Hayer to England to help gather evidence against Bagri, a plan it felt had potential to damage CSIS's operations, to harm CSIS's reputation and to put Hayer in danger by exposing CSIS's contacts with him. Despite these protests, when RCMP investigators travelled once more to England in 1988 for an "investigational trip" in relation to this scenario. CSIS was again kept in the dark and not told about the operation until a month afterwards, when the RCMP happened to need CSIS information for its own purposes.

Like opposing teams running in pursuit of the ball around a soccer field without goalposts, CSIS and the RCMP continued to actively pursue exclusive access to sources, without much clarity as to exactly what they thought they were trying to accomplish. A simplistic and inflexible view that CSIS was concerned with "intelligence" whereas the RCMP dealt with "evidence" led the agencies to approach their investigations mechanically. Without stopping to think about whether their "usual" methods made sense, both agencies as often as not ended up sabotaging their own interests as much as each other's.

3.9.2 CSIS: Refusal to Collect Evidence

The spectre of the abuses of civil liberties committed by the former Security Service and revealed publicly through the McDonald Commission continued to haunt the newly created CSIS. If nothing else, CSIS was determined to distance itself from scandal and keep within the four corners of its new mandate as it perceived it. There was a strong emphasis on limiting the information CSIS retained, as well as on avoiding the use of any "police-like" methods in collecting information. This strategy, which was plausible as a means to prevent repetition of past errors, soon became an end in itself as the new agency became mesmerized by the mantra that "CSIS doesn't collect evidence." This mantra was used to justify the destruction of raw material and information, even in cases where that material clearly implicated criminal activity and represented no more of an infringement of privacy than the summary reports CSIS did preserve.

At the same time, CSIS took an expansive view of its security intelligence mandate and seemed unable to resist the temptation of developing source "intelligence" – even when the information provided by sources was solely relevant to the question of who was responsible in the Air India case. The result was that throughout the Air India narrative, CSIS repeatedly took it upon itself to develop intelligence that went to the heart of the criminal investigation, with seemingly no regard for evidentiary requirements or thought for what would happen when the information ultimately ended up in a court of law.

CSIS continued to mechanically destroy its raw materials regardless of their content, a practice that came to have serious consequences for the Air India trial. When, in 1987, Ms. E told Laurie her story about Ajaib Singh Bagri's request to borrow her car the night before Air India Flight 182 crashed, Laurie followed the general practice at CSIS and destroyed the original notes and recordings he made in relation to his interviews. He did this, despite the fact that it was immediately clear to him and to his superiors that this was criminal information that would likely one day end up in court. Despite what he and his superiors may have believed, in doing so, he was not even going by the book. Up until 1990, the official CSIS policy dealing with retention of investigators' notes was still the old Security Service policy that required investigators to retain their notes where there was "reason to believe" that an investigation would "result in court appearances being necessary." Though still applicable, this was a policy that seems neither to have been known nor ever applied at CSIS.

At the Air India trial, Justice Josephson concluded that the destruction of Laurie's notes and audio recordings of his interviews with Ms. E violated Bagri's rights under the *Charter*. He then found that Laurie's reports about Ms. E's statements were admissible, but were not sufficiently reliable to support a conviction, since they were not meant to provide a complete record of his interactions with Ms. E or of all the statements she made, because CSIS "does not collect evidence."

CSIS's cavalier attitude towards the "evidentiary process" opened up the possibility that its investigations would ultimately compromise the RCMP's evidentiary position at trial. Even though CSIS appeared to recognize that the problem of "contamination" of the RCMP's Air India investigation could be an issue, it proved unable to take effective steps to avoid it. Laurie was instructed not to task Ms. E with any actions and not to question her specifically on criminal matters, but he was not told to stop meeting with her. Every time he did meet her, the topic of Air India ended up becoming the central issue discussed. Inconsistencies developed in the numerous reports Laurie created about what Ms. E told him during their meetings, and these ultimately served to weaken the Crown's case. The independence of Ms. E's recollection also became a concern, based on suspicion that Laurie may have provided information to her during their meetings - a suspicion that was difficult to refute at trial over ten years later in the absence of complete notes or recordings of the meetings.

Whether because of its more effective methods in approaching sources or because of the natural advantage it enjoyed in not being "the police," CSIS succeeded in obtaining a larger quantity of information, and more valuable information, from human sources than did the RCMP during the post-bombing period. It then proceeded to render that information essentially useless for the purpose of bringing the perpetrators for the bombing to justice as a result of its stubborn and unreflective insistence on not collecting "evidence."

3.9.3 RCMP: Refusal to Collect Anything But Evidence

Running parallel to CSIS's unhelpful insistence on not collecting evidence was the RCMP's insistence on not collecting anything but evidence. In relation to sources, this meant that the RCMP tended to assume that they were important only to the extent that they were willing and able to become witnesses and that their information was valuable only to the extent that it could be used as admissible evidence.

This attitude helps to explain the singular ineffectiveness of the RCMP in developing sources and its corresponding ability to squander the opportunity to elicit information from the sources that CSIS ended up turning over to the RCMP.

It should have been clear from the outset that if perpetrators of the bombing of Flight 182 were to be brought to justice, the authorities would have to rely on information from sources in the Sikh community. Though the forensic evidence about the bombing lay beneath the depths of the Irish Sea, there was a widespread belief that members of the tight-knit Sikh community knew who was behind the crime. These were circumstances that called for patient and sensitive approaches to members of the Sikh community, in the hope of drawing out the information that could piece together the conspiracy and point to the evidence that would be needed to make out the case in court.

The RCMP proved entirely incapable of meeting these challenges. Instead of emulating the successful methods of CSIS source handlers, the RCMP adopted an aggressive, insensitive and sceptical approach to potential sources of information which served to turn them away and render them uncommunicative rather than encouraging them to be forthcoming. Given this approach, it is not surprising that, when several of the CSIS source handlers who had developed promising sources in the Sikh community for CSIS transferred back to the RCMP, none were kept on in a parallel capacity at the Force, nor were they brought into the police investigation of the bombing.

The RCMP tended to take a linear approach. The predominant view was that, in light of the magnitude of the Air India tragedy, individuals with important criminal information were duty-bound to cooperate with police. This led the RCMP to approach sources in an aggressive manner, with a sense of entitlement. This approach was particularly ineffective in dealing with sources afraid for their safety. Members of the Sikh community were often reluctant to cooperate with police, both because of cultural assumptions about the police that were rooted in the Sikh experience in India and because they were fearful of the consequences of "collaboration" with the police for themselves and their relatives if their cooperation was discovered. It did not help that a man (Balbir Singh Kaloe) was believed to have been killed at the hands of Indian authorities as a result of information supplied to India by Canadian authorities. The RCMP's seeming blindness to the continuing threat of Sikh extremism, and the effect it had on the community, was in line with its narrow view of its role

and its lack of curiosity about the people or the culture it was dealing with. When CSIS investigators tried to explain to RCMP members the nuances of the Sikh community – including community attitudes towards the Sikh separatist movement, Sikh extremism and the bombing - they showed little interest, and a good deal of impatience with information they did not see to be relevant to their immediate criminal investigation.

This lack of understanding by the RCMP of the Sikh community compounded its problems in recruiting sources, and its approach turned sources into adversaries.

In the case of Ms. E, despite knowing that she was potentially suicidal and feared that if she cooperated with police, she and her children would be murdered, the RCMP made repeated, public, and aggressive approaches to her. Officers constantly dropped by her residence, where she worked with other employees, and spoke to her about Air India, at times within earshot of others. They made repeated suggestions about the "unpleasant things" that could happen if she did not disclose the full extent of her knowledge, even suggesting that if she failed to respond to a subpoena she would be arrested. They constantly referred to her alleged affair with Bagri in an accusatory manner, and even spoke to Ms. E's common law husband in a manner that led him to believe that Ms. E had had an affair with Bagri while already living with him. Determined to obtain a useable statement from her, the RCMP asked Ms. E to come to RCMP HQ, where she was interviewed for almost six hours, leading her to believe, as she later claimed, that she would not be allowed to leave until she provided a statement.

The impact of this bull-headed approach was counterproductive. Ms. E eventually sought psychiatric help, alleging that "…the police were putting words in her mouth and making her sign documents," a statement hardly likely to improve the credibility of any statements the police would subsequently seek to rely on in court. Undeterred, the police continued to drop in on her even after she retained a lawyer and required the RCMP to go through him.

While the safety of its sources should have been of the utmost concern to the RCMP, it often displayed a seemingly callous attitude towards its sources and resented their reluctance to help. In response to CSIS concerns about the inherent risk of the plan to send Tara Singh Hayer to England in order to have him gather evidence about Bagri's purported confession, the RCMP retorted that Hayer was a "grown man" and could make his own decisions. When Hayer changed his mind about participating in the plan, deciding not to act as an agent for the RCMP, some RCMP members interpreted his decision as an indication of his being unreliable and opportunistic.

The RCMP's approach to sources was heavily influenced by its hyper focus on "evidence". In contrast to CSIS, which felt intellectually compelled to pursue each interesting piece of "intelligence", the RCMP viewed its mandate as limited to the pursuit of "evidence." In practice this meant that the RCMP tended to lose interest quickly in information that did not seem potentially useful as evidence for securing a conviction in court.

RCMP Officers flew to India to meet with Pushpinder Singh, the ISYF leader who, at the time of the bombing, had been described as "one of the most important Sikh terrorists in the world," and who was alleged to have stated at the Khurana meeting two weeks before the bombing: "Wait two weeks and something big will happen." Once there, they concluded that any statement Pushpinder Singh was likely to make would be "totally exculpatory." On that basis they decided not to attempt to take a statement from him and for the time being to take no further action.

The deep suspicion of human sources, which was probably the result of the RCMP's routine dealings with the criminals and jailhouse informants who made up its usual sources, could lead to a premature dismissal of information based on preliminary assessments of credibility. Human sources who were looking to exchange information for a benefit were treated with special disdain, in part perhaps because of the RCMP view that witnesses should come forward out of a sense of civic duty and in part, no doubt, because such information is potentially vulnerable to aggressive cross examination when tendered as evidence in court. On the other hand, the information might just be true.

Time and again in the Air India investigation, the RCMP came down on the side of scepticism based on a superficial assessment of credibility, which led them to dismiss information long before its truth could reasonably be assessed.

When Person 1 provided information to the RCMP in the pre-bombing period about a plot to bomb an Air India plane, his information was quickly discounted, as investigators assumed that he was providing it only to further his own personal interests. This suspicion persisted even after the bombing, and in spite of the fact that the same information had been reported independently by another individual. It took months before the RCMP finally followed up with Person 1, whose information was ultimately verified by a polygraph examination.

In the case of Ms. E, before finally deciding to pursue her remorselessly to get her to testify, the RCMP had repeatedly found reasons to discount her value as a source of possible evidence. At first, though they believed her to be Bagri's mistress, the RCMP assumed that Bagri was unlikely to have discussed anything of importance with her. Later, officers cited her reluctance to admit her alleged affair with Bagri and her fear that it would be made public, as well as her unwillingness to testify as reasons to discount her. It was not until other RCMP investigators approached her by coincidence as part of a source development project in 1991 that the RCMP began to warm to the idea that she might be a useful witness. Despite the inconsistencies in her statements noted by the RCMP during its sceptical phase, she would ultimately become the Crown's key witness against Bagri at trial.

In yet another example of the RCMP's pursuit of "ready evidence," after the RCMP fought for months with CSIS over access to Mr. A, RCMP officers finally got the opportunity to meet with him. Then, after speaking to him for 15 minutes, during which he claimed that he had no "direct knowledge" and said he was

concerned for his safety, the officers wrote him off as having no immediate value to the investigation and concluded that no further follow-up in relation to this source was required at E Division. The RCMP did not consider the possibility that using Mr. A to develop intelligence could open doors in the investigation that might allow the potential gathering of evidence in the future.

Part of the RCMP's reluctance to deal with Mr. A was also based on a perception that he was an "opportunist," as he would not disclose the full extent of his information without a benefit for himself. Whereas the RCMP often engages in negotiations with, and provides benefits to, informants involved in criminal activities, it seems that in the counter-terrorism context, the RCMP expected that sources with criminal information would act altruistically and freely disclose their information to police, without benefits to themselves and without regard to their personal safety.

A similar pattern can be seen in the RCMP dealings with Mr. G – an important figure in the Sikh extremist movement in 1985 – whom the RCMP suspected might have had information about the bombing. When Mr. G informed the RCMP he was willing to provide information, but not to testify, the RCMP decided that it could not consider providing any concessions to him unless he provided "…full and complete co-operation of an evidentiary nature." When in 1997, Mr. G agreed to testify, asking only for protection for himself and his family in exchange, the RCMP still held back, insisting that he first needed to provide a statement that could be evaluated by the Crown before any commitments would be made.

The RCMP's pursuit of "ready evidence," and lack of interest in what it viewed as "intelligence," seems to have led it to prematurely cut off avenues of investigation that could have led to a deeper understanding of the Air India conspiracy and the persons involved. On August 26, 1988, Hayer was the victim of a vicious attack that left him in a wheelchair for the rest of his life. Harkirat Singh Bagga visited the Indo-Canadian Times office and shot Hayer three times. Bagga initially identified Bagri as having put him up to the crime, but later retracted his statements and pled guilty to the crime. RCMP investigator Solvason, as well as the Hayer family, expressed the view that there were other extremists who had put Bagga up to the shooting and that the investigation had an important national security dimension. However, there was no willingness at the E Division Air India Task Force to take the case on. Following an investigation by the Surrey Detachment, Bagga was convicted of attempted murder. It was the family's view that, at that point, the RCMP simply closed the file in relation to this matter. They testified that this decision was emblematic of the Task Force's failure to see the bigger picture in relation to Sikh extremism. It was only in the late 1990s that the Air India Task Force finally got involved in the investigation of the Hayer shooting. Once the Task Force began looking to establish a motive for Bagri to have conspired with Bagga to murder Hayer, it discovered information showing that Hayer had publicly pointed to Bagri as responsible for the Air India bombing, even mentioning an alleged confession, shortly before the shooting.

3.9.4 Lack of Effective Source / Witness Protection

Not surprisingly, given the RCMP's failure to appreciate the continuing threat of Sikh extremism, it had a poor record in terms of responding to threats directed at both sources and potential witnesses in the Sikh community.

Of the three individuals who were to be the key witnesses at the Air India trial, one was murdered before the trial began, one feigned memory loss because she was too scared to testify about the knowledge she had previously claimed to have, and one was forced to enter the Witness Protection Program two years earlier than planned and felt that her life was ruined.

As with the other aspects of its dealings with Ms. E, the RCMP's response to her stated fears for her own safety and that of her family were insensitive and ham-handed. The RCMP had few effective strategies for dealing with reluctant witnesses who feared for their safety.

The RCMP speculated that Ms. E's reluctance to cooperate was more the result of concern that her alleged affair with Bagri would become publicized than of any genuine fear of a threat Bagri might pose to herself and her family. The irony of the RCMP's belief that Bagri was one of the key masterminds in the worst terrorist attack in Canadian history alongside its questioning of the genuineness of Ms. E's fears was apparently lost on its members. The same scepticism about her fears, combined with the familiar fear of compromising credibility by offering a "reward," would seem to explain the view expressed by the current head of the Air India investigation that discussing possible source or witness protection measures with Ms. E would have been premature until the RCMP had obtained statements about the full extent of her knowledge, since it was important to get the source's "evidence" prior to offering her any "incentives."

It was not until after the murder of Tara Singh Hayer, in November 1998, that Ms. E was informed of examples of specific safety measures that could be provided to her for protection, all of which she then declined.

At trial, Ms. E was ultimately left with the onus of personally applying for a publication ban on her name, with both Crown and defence taking no position in relation to the application. By this point in time, Ms. E was no longer on speaking terms with the RCMP. She was so concerned for her safety that she feigned memory loss, leaving the Crown with only the flawed reports written by Laurie through which to try to enter into evidence the information she had provided.

In some cases, the difficulty the RCMP experienced in appropriately responding to the threat to potential witnesses may have been the result of a lack of centralization in the RCMP investigation. This certainly appears to have been a factor in the lack of adequate protection for the identity of Ms. D, who was the Crown's key witness against Malik at trial. Ms. D initially approached CSIS with information about Malik in the late 1990s and was promptly turned over to the

RCMP. Some of her information related to frauds at Malik's Khalsa School, which the RCMP decided to refer to its commercial crime section while the Air India Task Force continued to stay in contact with her. The commercial crime section, perhaps unaware of the nature of Sikh extremism and seriousness of the threat faced by Ms. D, allowed Ms. D's name to be released when it inadvertently left a warrant application in connection with its investigation unsealed. Once the fact that she was providing information to the RCMP was revealed publicly, Ms. D had to enter into the Witness Protection Program over two years earlier than would have otherwise been necessary, exacerbating the disastrous impact that the Witness Protection Program has had on her life. Ms. D felt that her "whole life [was] ruined," as she lost the opportunity to watch her eldest son grow up and her youngest son lost the opportunity to be with his brother and father.

Serious as these failures undoubtedly were, nowhere are the RCMP's failures to protect its potential witnesses more dramatic than in relation to Tara Singh Hayer. Hayer's family testified as to the difficulty in getting the RCMP to take threats against Hayer seriously, even after two attempts had been made on his life. When Hayer provided the RCMP with a letter containing threats against him, the RCMP became fixated on an analysis of whether "overt threats" were being made as the basis for assessing the seriousness of these threats, an analysis reminiscent of the similarly undue and mechanical reliance placed by government agencies on the concept of "specific threat" to explain away the importance of pre-bombing threat information. Despite the statement "…[s]ometimes I think what a big mistake he did who just made you handicapped. Well that's okay there is delay but not darkness at God's house," and despite the reference to big "punishment", the RCMP concluded there were no overt threats in the letter and thus nothing further needed to be done. It took the intervention of the Ministry of the Attorney General of British Columbia (BC) to get the RCMP to take action.

This, apparently obtuse, initial response to the threat against Hayer may in part be explained by the fact that, because there was no centralized coordination of threat information, the unit that first dealt with the threat was unaware of previous threats to Hayer or of the fact that Hayer had in the past been the subject of a murder attempt. While this may serve in some measure to explain the response, it also demonstrates the inadequacy of RCMP information management about threats. Indeed it appears that, rather than centralize and coordinate such information, the RCMP practice was often to purge it from the records.

The RCMP had difficulty providing Hayer with protection while respecting his autonomy. Hayer was committed to continuing his journalistic work and thus he did not consider entering a witness protection program to be a viable option. The RCMP invoked resource constraints to explain its inability to provide Hayer with constant personal security, apparently believing that there was no other alternative that could have kept Hayer safer while allowing him to continue living his life as normally as possible.

After a period of escalation of threats, and after Hayer's name appeared on a "hit list," the RCMP finally installed video surveillance at Hayer's residence in July 1998. But the equipment installed was totally inadequate. Because of a unilateral RCMP decision not to drill holes in the residence, the equipment ceased working when its antenna was not kept in a particular position. To make matters worse the Hayer family was not informed of this fact, and was unaware of the steps necessary to ensure that the equipment would function properly. When Tara Singh Hayer was brutally murdered in his garage in November 1998, the equipment was not functional. Only "snow" was recorded on the video cassette and no footage could be recovered. Prior to appearing as witnesses before this Inquiry, Hayer's son and daughter-in-law were unaware that the video surveillance system had failed. When in the past the family had asked the police if they could view the surveillance tapes, they had been told that this was not possible due to the "ongoing investigation." The murder of Hayer occurred ten years ago. The individuals responsible have still not been identified and brought to justice.

The final accounting of what occurred in relation to these three key human sources of information about the Air India bombing is disturbing. In light of the RCMP's woeful failure to protect these and other individuals, along with its mechanical, aggressive and uncoordinated approach, it is no wonder that the RCMP experienced significant difficulty in penetrating the Sikh community. There is a reasonable limit to how much any individual citizen can be expected to sacrifice in support of the pursuit of justice.

3.10 RCMP Investigation

The RCMP has long insisted that, though the security intelligence function was transferred to CSIS, it had to maintain responsibility for, and control of, national security *criminal* investigations. The RCMP pointed to CSIS's lack of mandate and lack of expertise in the conduct of criminal investigations as a prime reason why the RCMP should be involved in cases involving potential criminality early on, and why the RCMP should take over the investigation of all criminal offences involving national security, such as terrorism.

However, when the RCMP did become responsible for the Air India criminal investigation, the challenge of uncovering and bringing to justice those responsible for this unprecedented act of terrorism proved more difficult for the Force than perhaps had been expected. Conducting this terrorism investigation with international ramifications necessitated working without the ready availability of forensic evidence about the crash of Flight 182, and required the gathering of intelligence in a community and about a phenomenon not well known to the RCMP or well understood by its officers.

Rather than adapting its approach and methods to the unique national security aspects of the case, the RCMP maintained its traditional focus on obtaining ready "evidence" and applied a rigid standard of credibility or evidentiary value to potential investigative leads.

The RCMP was unable to suspend the evaluation of the information it compiled until it had accumulated a meaningful amount of information from various sources and instead prematurely discounted information, such that it was never able to accumulate enough pieces to complete the puzzle. Very early on in the investigation, the RCMP developed a theory of the case, and from then on quickly discounted potential leads or pieces of the puzzle that did not appear to fit.

Overall, the RCMP was unable to incorporate an intelligence-based approach to the investigation.

3.10.1 National Security without Intelligence Gathering

From the outset of the Air India and Narita investigations, the RCMP's view was that there had been one plan to execute two concurrent acts of terrorism against the Indian government, in which the key participants were Parmar, Bagri, Gill, and Johal – with Inderjit Singh Reyat used in the plot for his bomb-making expertise and access to materials. Given the results obtained in Narita – which had a readily available crime scene and in which Reyat was ultimately convicted for manslaughter only – it should have been clear to the RCMP that in order to get to "the brains" of the operation, something more than a purely forensic or "yellow tape" crime scene-oriented type of investigation was needed.

However, challenges were encountered from the beginning. Even assembling the E Division Task Force to investigate the bombing was difficult. Not only did Federal operations RCMP members lack experience in homicide or other major crimes investigations, but investigators generally had no training in the area of terrorism/extremism investigations, no understanding of Sikh extremism, and only one or two members could speak Punjabi.

RCMP management was unsupportive of the type of investigative initiatives that would have been required to investigate such an exceptional case. When investigators suggested a re-orientation of the investigation towards a conspiracy approach or attempted to engage in intelligence-connected endeavours – such as source development and strategic prosecutions – management was unable to appreciate the value of these pursuits and actively discouraged the initiatives.

The perceived difficulties in solving the Air India bombing led the RCMP to devote fewer resources, rather than more, to the investigation, and it increasingly focused its resources and energy on Narita. By the late 1980s, the Air India file at E Division was being handled by a unit for which the investigation was one assignment among many others. At one point, it was assigned to a single person, who coordinated recovery attempts of the wreckage of Flight 182 and took care of file administration. There was a formal attempt by E Division management to shut down the Air India investigation. Not surprisingly, morale became a very serious issue and the work environment became "poisoned."

Structurally, RCMP decentralization made it difficult for the Force to achieve central coordination of the investigation and to see the broader picture emerge. RCMP Divisions were not accustomed to involving HQ in operational decisions and HQ personnel had no formal line authority over members in the Divisions. "Directives" issued by HQ were generally taken as suggestions and were often unwelcome. The Divisions only informed HQ of what they thought HQ should know. Answers to HQ's questions, when and if they were provided, were often superficial.

With this structure and approach, the RCMP was frequently unable to recognize the value of the information in its possession. Often, RCMP investigators simply could not access all the pieces in the RCMP's possession because of the manner in which the information was filed. There were ultimately numerous and extensive file reviews, but no ongoing summary of the Air India file was created. Investigators could not easily gain an overview of the file. With the high rate of turnover on the Task Force, maintaining continuity in the investigation was difficult. The filing system itself did not help put information together. Due to the multiple filing systems across the country, investigators had to search multiple databases – sometimes in different geographic locations – to find all the relevant information. Given the difficulties in storing and retrieving information, important information was at times misplaced, lost, and even destroyed.

Even when information was accessible, the lack of an intelligence orientation in the investigation meant that no one even thought to access it. The information accumulated by the RCMP in the pre-bombing period about threats to Air India, about the individuals who were likely to attack Indian interests in Canada and about the modes of attack that were possible, was never accessed in the post-bombing period. As a result, the June 1st Telex – which provided information about the June 1985 threat of sabotage with time-delayed devices concealed in luggage – was never looked into by the Air India Task Force, nor were its origins investigated.

Even when RCMP investigators did find new information and began to examine it, the information was often discounted – precisely because so many other pieces of the puzzle which had been uncovered before had already been discounted, lost, or buried in files that were never reviewed.

Very little progress had been made in the investigation by the early 1990s. Current Deputy Commissioner Gary Bass was asked in 1995 to examine the investigation that had been done to date and to advise whether there was anything else that could be done in the investigation, which had seemingly reached an "impasse." He decided to re-orient the investigation towards a conspiracy approach, place experienced members on the file, create a dedicated task force, and implement new intelligence-led investigative strategies. The investigation, and the ultimate decision to take the matter to prosecutors, proceeded largely, and at times exclusively, on the basis of information that had been in the RCMP's possession all along, but which was finally being examined in a new light. What could have been done 10 years before was finally done in 1995. Some of the information

dismissed by the RCMP over the years in its pursuit of its primary theory of the case continues to raise questions to this day.

3.10.2 Premature Dismissal of Intelligence and Theory of the Case

The RCMP demonstrated an insufficient ability to recognize the significance of intelligence or to correlate all the relevant information. As a consequence, the RCMP deprived itself of a great deal of important additional information, as it made decisions to delay or not to follow up on leads and continued to discount the value of some of the information it was receiving. Assuming, as the RCMP has certified, that the Commission has been provided with all relevant documentation, the RCMP's follow-up investigation in relation to a number of leads raises questions.

Within the first few months of the investigation, the RCMP developed a theory of the case in terms of the main suspects, the motive, and the modus operandi of the crime. By August 1985, the RCMP's investigative efforts were focused on demonstrating that the Air India bombing had been perpetrated by the Babbar Khalsa (BK) – masterminded by Parmar, with the assistance of Bagri, Gill, Reyat and Johal.

However, immediately after the bombing, the RCMP suspected the involvement of members of the International Sikh Youth Federation (ISYF) – an historically violent organization that had been proscribed in India because of its bombing assassinations of Sikhs and Hindus. The ISYF was one of the three organizations that had claimed responsibility for the attack on Air India Flight 182. Members of the ISYF had been present at the June 12, 1985 meeting at the home of Sarbjit Khurana, where ISYF leader Pushpinder Singh was alleged to have commented that something big would happen in two weeks to show the Indian government that they were serious. Khurana reported the information about the "wait two weeks" comment allegedly made by Pushpinder Singh to Vancouver Police Department Detective Don McLean immediately after the meeting, approximately two weeks before the bombing, and McLean had no doubt that Khurana had been telling the truth.

The RCMP initially focused its efforts on the surveillance of ISYF members who had been present at the Khurana meeting. Extensive coverage of Lakhbir Singh Brar, another ISYF leader who accompanied Pushpinder Singh to the Khurana meeting, began by the RCMP in late June 1985. However, in mid-August 1985, the RCMP decided that its focus on Lakhbir Singh Brar should be discontinued and efforts re-focused on Parmar and associates since Lakhbir Singh had not demonstrated any involvement in criminal activity. The RCMP theory that the Air India bombing was an act of the BK alone soon became firmly entrenched. From that point on, information implicating other groups or individuals not seen to be directly connected to Parmar and his BK associates was often consigned to the RCMP's category of "alternative theories" and was not intensively pursued.

The view that the Air India bombing was an act of the BK alone appeared to affect the RCMP's follow-up on the Pushpinder Singh comment, in spite of its clear intelligence value and even though the involvement of the BK in no way excluded the possibility of ISYF involvement. In fact, Khurana had reported that, during the meeting at his residence, Pushpinder had praised Parmar, had said that he had met with him the previous week, and had indicated that he was using him to bring all Sikhs in the lower mainland together. The persistent refusal to explore the possibility that other organizations, such as the ISYF, had worked in conjunction with the BK is difficult to understand in light of the fact that, in the course of subsequent RCMP investigations into terrorist plots involving the Babbar Khalsa in 1986, the RCMP became seriously concerned that the BK and ISYF had been consolidating their efforts within Canada and had been working together in furtherance of their separatist goals.

When an RCMP HQ analyst showed interest in Pushpinder Singh and raised questions about the possibility that the BK and ISYF had worked together in relation to the Air India bombing, the response of E Division was dismissive and even hostile. E Division complained in effect that HQ was wasting its time with fanciful theories.

The RCMP's efforts to follow up on the Khurana information after the bombing were heavily and inexplicably focused on pursuing an exact translation of the Khurana tapes that would verify the alleged comment. Early RCMP translations of the Khurana tapes, which were based on extremely poor quality of recording, had revealed portions of conversations containing ominous remarks, including the comment that "…it may take two weeks, a few months, or a few weeks and then we will do something…." In spite of these early translations, which appear to support Khurana's statement, the RCMP seems to have simply accepted CSIS's view that the only conversation of interest on the tape was about the goal of bringing Sikh groups together. The RCMP later flatly told Rae that the "wait two weeks" comment had not been recorded. No mention was made of the early RCMP translations.

The pursuit of any possible ISYF connection had become so low a priority after the re-orientation that, aside from the early surveillance, no follow-up to determine Pushpinder Singh's possible involvement in the Air India bombing had been commenced by the RCMP over a year after the bombing. When the RCMP learned that Pushpinder Singh had been arrested in India in early 1987, no attempt was made to interview him at that time; on the basis that such action was deemed to be "premature." When an RCMP team traveled to India in January 1988, Pushpinder Singh was finally interviewed. The interview consisted of asking him, point blank, for information about his knowledge of, or responsibility for, the Air India bombing. When Pushpinder Singh, not surprisingly, displayed an apprehensive and defensive attitude, the Force concluded he was not forthright and stopped pursuing the matter. Pushpinder Singh offered to take a polygraph about his involvement in the Air India bombing, but the RCMP did not follow up because of the difficult logistical arrangements that would have been necessary in India and, remarkably, because it was felt that he might well

have passed the test. Very little investigation took place over the next seven years. It was not until 1995, when the file was reviewed in preparation for the 10-year anniversary of the bombing and a revived Task Force was constituted, that further investigation of Pushpinder Singh's possible role took place.

So complete was the RCMP's dismissal of a possible ISYF connection in relation to Air India that, prior to 2001, Lakhbir Singh Brar had never been interviewed as a potential witness or suspect regarding Air India, despite his frequent association with Babbar Khalsa suspects, despite the fact he had been involved in the Khurana meeting, and despite the RCMP's initial focus on his activities.

In May 1997, the RCMP received information that called into question the official version of the circumstances surrounding Parmar's death in India in 1992, which was originally reported to have been the result of a "shoot out" with Indian police. The new information revealed the existence of a confession that was purported to have been made by Parmar prior to his death. The RCMP received information from a number of sources that Parmar had died while in the custody of the Punjabi police who had interrogated him and extracted information about his activities, including some information about the Air India bombing. The sources told the RCMP that Parmar had indicated that the identity of Mr. X, the third individual who had accompanied Parmar and Reyat to the Duncan Blast site, was Lakhbir Singh Brar – a member of the ISYF, and that Lakhbir Singh had also purchased the ticket in the name of "L. Singh."

Lakhbir Singh was finally interviewed by the RCMP in 2001, when he surfaced as an applicant for Canadian immigration in Pakistan. The RCMP did not interview him solely because of the purported confession. Indeed, Lakhbir Singh was "… well on his way to elimination [as a suspect by the RCMP] before these interviews took place." Investigators felt that the information contained in the purported Parmar confession was problematic in that it did not accord with information the RCMP already had on file. Much emphasis was seemingly placed on information investigators had about Lakhbir Singh's age, which was felt to be incompatible with the observations that the CSIS surveillance team had made of Mr. X during the Duncan Blast. According to the RCMP's information, Lakhbir Singh would have been 33 years old at the time of the bombing. Information uncovered by the Commission called into question the RCMP conclusion about Lakhbir Singh's actual age. Certainly, the extent of reliance placed on conclusions arising from CSIS surveillance information was questionable given the multiple instances in the pre-bombing period of misidentification by CSIS of individuals of a different race from their own.

The RCMP's "evidentiary" focus also meant that the RCMP's initial assessment that Person 1 and Person 2 lacked credibility was used to justify its failure to follow up or even adequately to report information about the November Plot in the pre-bombing period. After the bombing, the scepticism continued, and this meant that the RCMP failed to follow up on the information in a timely way despite the potential connections with the Air India bombing. The RCMP viewed this matter as totally unconnected to the Air India case, and dealt with

inquiries about it as merely tying up "loose ends," for purposes of confirming the main theory of the case. HQ sent information requests aimed at exploring the possibility of a connection, but E Division often simply failed to answer.

Of course, it was only by investigating the information as it presented itself that any connections with the Air India bombing could have been discovered. It was no surprise that such connections were later discovered when HQ finally received from CSIS the information E Division failed to provide about Person 2's associates: at least one of whom had connections to the Babbar Khalsa. Telephone records reveal that calls had been made from the home of Person 1 to Inderjit Singh Reyat, the Air India bomb-maker, the day after Person 2 was arrested in October 1984.

It was not until media reports in 1986 described the November Plot information as a forewarning of the Air India bombing that the RCMP had received and ignored, that the investigation into this matter truly began in earnest. Even when RCMP analysts did begin to recognize the potential relevance of the November Plot information and the significance of the fact that the information had been provided by two separate sources prior to the Air India bombing, the follow-up investigation continued to be tainted by the initial RCMP assessment that the information lacked credibility and by the view that any November Plot connection did not fit with the RCMP's theory of the case.

When the RCMP began to make inquiries about "Z"[1], who had been identified by Person 1 and Person 2 as having potential involvement in the November plot, it was learned that he had departed Canada for India and had not since returned. In 1988, "Z" was charged in an unrelated matter and arrangements were made for him to provide a polygraphed statement about the November Plot in exchange for a reduction in his sentence. He provided an exculpatory statement. Although the RCMP told Rae that "Z"'s polygraph "verified" his information, the Commission discovered in the course of this Inquiry that Z's polygraph examination had, in fact, been inconclusive in part. Despite the fact that the test was incompatible with Person 1's polygraph test, which he passed in its entirety, the RCMP concluded that "Z" was not involved in the Air India bombing.

When the RCMP began to investigate the possible involvement of "W", an individual identified by Person 2 as having had possible involvement in the plot, and identified by Person 1 as likely having been responsible for the calls made from his home to Reyat, it emerged that "W" had been involved in the past with Parmar, Gill, and Reyat, the RCMP's main suspects in the Air India bombing. "W" was a member of the ISYF and admitted to the RCMP that he would be willing to "do anything" to avenge the death of his relatives in the Punjab. He also told police that, in the past, he, Parmar and Gill had been planning on "doing something" in India. In spite of this startling information, it is not clear what, if anything, the RCMP did to further pursue the possibility of "W's" involvement.

---

1 This is not the same individual as "Mr. Z", a CSIS source who also provided information to the RCMP.

Perhaps because of the difficulties it experienced in managing an investigation of this magnitude, the RCMP sometimes prematurely discounted or failed to follow up – even on information that was consistent with its principal theory of the case. When Tara Singh Hayer provided information in 1986 about Bagri's alleged confession in England that he had been responsible for taking the bomb-laden luggage to the airport, Bagri became an important RCMP suspect. Nevertheless, the RCMP did not go back to pursue Ms. E, whom investigators had identified in 1985 as potentially being Bagri's mistress. The RCMP also did not pursue CSIS's cryptic references in 1987 to a Vancouver source who had been approached by Bagri to borrow her car and take it to the airport the night before the bombing. In 1989-90, during the Watt MacKay file review, this information was finally re-evaluated, leading the RCMP to understand that the person in question was Ms. E.

Information received from Mr. Z in 1986 about individuals connected to Bagri who were identified as potentially having involvement in the delivery of the luggage on Bagri's behalf was not followed up until 1987. Even then, the follow-up was less than enthusiastic. The 1987 investigation of Mr. Z's information consisted of having officers observe the individuals named by Mr. Z and compare their appearances to the composite of "M. Singh," that had been created by the RCMP on the basis of information provided by Ms. Jeanne ("Jeannie") Adams, the check-in agent for CP Air in Vancouver. They concluded that the suspects did not match the drawing.

The RCMP's quick discounting of the Mr. Z information is puzzling for a number of reasons. The currently accepted theory is that two individuals, the so-called "M. Singh" and "L. Singh" were responsible for checking in the luggage containing the explosives on June 22, 1985. Adams was only able to recall the check-in of "M. Singh," and thus could not provide information about L. Singh's appearance. To discount the possible involvement of individuals on the basis of a composite for only one of the two suspects seems unusual. It's also unclear how much reliance should have been placed on the "M. Singh" composite produced by the RCMP. Though Adams had provided a number of different descriptions to the RCMP, she also stated that she did not recall the suspect's face. More importantly, she said the composite drawing that the RCMP had produced was not correct.

Even more remarkably, the factor used to rule out the suspect - two years after the events and on the basis of comparing his appearance to an imprecise drawing - was the observation that he was "different by his hair," as it appeared to be combed straight back, and was "not wavy and not parted on the left side." After making these observations, officers concluded that there would be no further investigation of the file unless CSIS provided further information to substantiate the Mr. Z information.

In early 1988, the RCMP met with some (but apparently not all) of the individuals identified by Mr. Z as having possible involvement. Again, the RCMP discounted the potential involvement of these individuals on the basis of the "M. Singh" composite, as well as on factors such as the level of English spoken by the suspects.

Though at least one suspect had indicated a willingness to be polygraphed, none was asked to undergo a polygraph test and these "interviews" apparently put an end to any follow-up investigation in relation to the Mr. Z information. The interviews were taped, but the tapes were destroyed for unknown reasons and no transcripts were ever made. No further investigation of this matter was conducted until close to a decade later, at which point some of the suspects were finally subjected to polygraph examinations.

The RCMP's approach to its post-bombing investigation must be kept in mind when evaluating the Force's strong criticism of CSIS and of its failures to share information post-bombing. The manner in which the RCMP conducted the investigation, both in terms of its relationship with sources and its follow-up on leads, might naturally be expected to have an impact on CSIS's willingness to share information. At the same time, this consideration does not exonerate CSIS in its information-sharing practices.

3.11 The Sharing and Use of CSIS Information

The Air India investigation raised the question of the limits to the protection that CSIS information could legitimately receive in the face of the imperative of prosecuting those involved in the murder of 331 persons. Too often, information-sharing disputes prevented a proper balancing from being properly carried out, as CSIS and the RCMP debated everything except the real issues. The RCMP experienced frustration because of CSIS's refusal to provide information based on legalistic distinctions between "raw material" and "information" and its practice of answering RCMP questions in the narrowest manner possible. CSIS, meanwhile, was unable to gain any comfort that its sensitive information would not be made public by the RCMP. Each agency exaggerated the public interest that corresponded to its particular interests, with the RCMP generally claiming that every piece of information was essential to the investigation and CSIS often taking the initial position that disclosing the requested information was too dangerous to its operations. Too often, no real analysis was conducted on either side and the agencies came to have little respect for each other's broad claims and assertions.

3.11.1 Early Access to and Use of CSIS Information

CSIS did not, as a matter of policy, retain the tapes made from intercepted communications, and routinely erased them following translation and transcription. By July 1985, the RCMP was aware that CSIS had been intercepting Parmar's communications since before the bombing, and the Task Force requested direct access to the materials at that time. Although the RCMP continued to seek access to the tapes, and the Crown counsel assigned to the investigation directed the RCMP to seek their retention, the Task Force did not make a written request to CSIS for the preservation of the tapes. The erasures of the pre-bombing intercepts continued. Indeed, CSIS continued to erase the tapes of its ongoing post-bombing intercepts of Parmar's conversations until the Department of Justice ordered a stop to the erasures in February 1986.

While the RCMP Task Force obtained access to CSIS reports containing summaries of the available intelligence during the early days of the investigation, requests for raw data such as underlying surveillance reports, interview notes, or intercept logs were generally met with resistance by CSIS. Continuing policy debates at CSIS about the terms and extent of RCMP access resulted in a "revolving door" of changing rules, marked by intermittent access punctuated by abrupt interruptions and long periods without access to any information.

An RCMP affidavit in support of an application to intercept the communications of Parmar and other key Air India suspects was sworn on September 19, 1985. It made extensive use of CSIS information and also made reference to the problems experienced by the RCMP in gaining access to CSIS materials. Use of CSIS information in warrants raised the possibility that these warrants would be challenged in court in such a way as to expose the CSIS information publicly. CSIS reacted to the use of its information by revoking RCMP access to the Parmar logs and by placing additional restrictions on access to its information. When the RCMP wanted to use CSIS information in support of a search warrant application, CSIS stipulated that the RCMP had to hide the fact that CSIS was the source of the information, which raised concerns that the RCMP's legal position in any eventual prosecution could be compromised, given the legal need to be forthcoming in warrant applications.

It was not until October 1985 that the RCMP learned that CSIS had erased the tapes on which its Parmar intercept logs were based. It was only in December 1987 that CSIS formally acknowledged that the Parmar tapes had been destroyed, and it would be years before the question of why the tapes were erased – and of whose responsibility it had been to ensure their preservation – would begin to be answered.

Over time, the back and forth recriminations between CSIS and the RCMP distorted perceptions and led the RCMP to take the position that, due to a lack of information about CSIS's investigation, the Force focused its early investigation on, and obtained intercepts on, the "wrong targets." According to this revision of history, without access to CSIS intercepts, the RCMP did not know that Parmar was to be a primary suspect. This is not the case. The RCMP was aware of Parmar as a prime CSIS target early in July 1985, and even had access to reports containing some of Parmar's conversations, that it later viewed as providing key indications of his involvement in the conspiracy. The debate was not about a lack of awareness of CSIS information, but about the ability to access and use "raw" information contained in the CSIS translators' notes and intercept logs in support of RCMP warrant applications or prosecutions. This confusion demonstrates precisely the muddling of the issues of access and use that plagued the agencies' relationship throughout.

3.11.2 The Reyat Trial and Beyond

Between July 1985 and October 1991, James Jardine (now a judge of the Provincial Court of British Columbia) was the Crown Counsel involved in the

Air India and the Narita investigations. He was involved in the prosecution of Parmar and Reyat in connection with the Duncan Blast charges and later in the prosecution of Reyat in connection with the Narita bombing. He transmitted numerous requests to the RCMP for access to CSIS information, including requests for explanations about CSIS policies and procedures for the processing of the Parmar tapes as well as a reliable accounting of their destruction. Jardine testified that CSIS's relationship with him was not open or cooperative, and that CSIS was not forthright.

Jardine was worried about the possibility of defence challenges to the search warrant used to seize key items of evidence from Reyat's home, given that the warrant application relied on CSIS information but concealed CSIS's role as a source. He was also concerned about potential abuse of process arguments being made by the defence because CSIS's erasure of the Parmar tapes made it impossible to disclose this possibly relevant material to the defence. The Crown would need to show that the erasures had been done innocently, and Jardine believed he required more CSIS information in order to do that. Despite numerous high-level meetings intended to resolve the issues, Jardine did not obtain the totality of the information he sought from CSIS until 1991.

In his March 1991 decision in the case against Reyat, Justice Paris stated that it was clear that the tape erasures occurred strictly as a result of the routine application of administrative policy and that there was no question of improper motive. However, in the Air India trial, Justice Josephson found, following a concession on the point by the BC Crown prosecutors, that the CSIS erasure of the Parmar tapes was unacceptably negligent. The evidence before the Commission justifies the latter conclusion, even though CSIS did not repeat its concession regarding this negligence in these proceedings

The Commission found no evidence that CSIS deliberately attempted to suppress evidence by erasing the Parmar tapes. Rather, CSIS personnel handling the Parmar intercepts seemed to have been operating in "default mode," erasing tapes regardless of their content and without any awareness of the applicable retention policies. Although these policies were somewhat vague, had they been applied they may have led to the preservation of at least some of the tapes.

With the tapes erased, only the translators' and transcriber's original notes were available to the RCMP. While CSIS continues to claim that there remains no reason to suspect that the erased tapes contained information about the planning of the Narita and Air India terrorist attacks, a review of the original intercept tapes would, at the very least, have yielded a better understanding of how Parmar employed coded language. Without the tapes, it is simply impossible to determine what information, if any, was lost due to the Parmar tape erasures or the potential importance of that information to the investigation and prosecution of the Air India and Narita bombings. It is clear that CSIS did not take the necessary steps to properly educate and train the translators and transcribers for this investigation, and this fact leaves the quality of CSIS's

analysis of the intercepts in a state of uncertainty. Even worse, as inadequate records were kept throughout the processing of the Parmar tapes, it remains uncertain whether all of the tapes were even listened to prior to being erased.

CSIS officials have pointed to the conviction of Reyat on manslaughter charges as a signal of success in the RCMP-CSIS relationship. If it was a cooperation success, it was one that was achieved only after a great deal of posturing and delay. Another success of sorts occurred at the Air India trial, where, despite the finding of "unacceptable negligence," at least the trial itself was not cratered by disclosure issues, though in the end the prosecution failed on other grounds. These "successes" should not be mistaken for an indication that the information-sharing problems between CSIS and the RCMP in connection with criminal prosecutions have been resolved, since they largely resulted from CSIS's view of the Air India prosecution as a special case, requiring it to derogate from its usual practices and policies.

In fact, problems of information sharing were present throughout the Air India narrative. CSIS failed to share information with the RCMP about important facts relevant to the police investigation, including, notably, its suspicions that Parmar – the RCMP's main Air India suspect - may have died in October 1992, after being captured, allegedly tortured, and killed in custody by Indian authorities. Its failure to share information also had significant logistical implications for the investigation. The RCMP only discovered in early 1996 that CSIS possessed over 200,000 tapes containing the intercepted communications of Parmar, Bagri, and Malik, among others, recorded between 1985 and 1996. As a result of this disclosure, the RCMP had to delay submitting its new wiretap application until it had reviewed 60,000 pages of intercept logs.

3.12 Overall Government Response to the Air India Bombing

Government agencies, in both the pre-bombing and post-bombing eras, often followed policies and procedures blindly, with no real sense of the concrete impact of their conduct and with little reflection about the goals they were pursuing or the best manner of achieving them. The result was that individuals and units within the Government performed their functions mechanically, often without co-ordination and without the imagination or flexibility necessary to enable the system to work in an effective manner.

Ironically in its responses to the victims' families, to external reviewers and to the public, the Government showed more coordination and a clearer sense of purpose than in its implementation of pre-bombing security measures and its investigation of the terrorist attack. Government agencies united to defend and justify their behaviour in order to avoid having to answer detailed enquiries about their processes, or to avoid having to make changes not of their own choosing. These goals were clear and were vigorously pursued with some success. As a result, an in-depth independent review of the terrorist attacks on Air India and an identification of deficiencies in the agencies' performance were inordinately delayed. A great deal of information was revealed to the public for the first time during this Inquiry, more than twenty years after the terrorist attack.

Notwithstanding the resistance to review, it cannot be said that the government agencies were attempting to hide any specific "smoking gun." In reality, although they reflexively adopted their defensive stances, for the most part the agencies did not know what they were hiding, or even whether there was anything to hide. They simply appear to have been trying to avoid public criticism, to avoid civil liability, and to avoid having to answer for their actions to independent or external reviewers whom they did not trust to pass fair judgment on their policies, practices and behaviour.

The positions taken by the government agencies over the years were effective in blocking a full public examination of the facts and circumstances that gave rise to the terrorist attacks on Air India as well as blocking any meaningful review of the investigation of the attacks. The families of the victims received practically no information or assistance, with the notable exception of the sensitive and elaborate mechanisms implemented by the RCMP Air India Task Force to liaise with and to provide support to the families of the victims over the course of the Air India prosecution. They received no answers from their Government and were often treated in a deplorable manner, while the government agencies continued to pursue the twin goals of deflecting public criticism and avoiding liability to pay compensation to the families.

3.12.1 The Government's Past Response

Defensiveness

From the very outset, the Government adopted a defensive stance. Within days of the bombing, direction regarding the Government position to be taken on the bombing was passed from the public service to political staff in the Prime Minister's Office. The result was that public statements were issued denying any mistakes and affirming the absolute adequacy of the security measures in place.

Defending the Government from potential civil liability to the victims' families soon became a priority. Instructions were issued to avoid any acknowledgement that the crash of Flight 182 was caused by a bomb, a fact apparently evident to the seamen recovering bodies on the fateful day. A preoccupation with avoiding any statements that might compromise the Government's ability to deny civil liability came to colour the interaction with the families of the victims who were treated more as if they were adversaries than victims.

Efforts were made to limit the funds expended to respond to their concerns. Families in financial need were essentially told to apply for welfare rather than expect compensation from Government. It was not until 1995 that the RCMP decided to hold meetings with the families to inform them about the status of the investigation. For its part, CSIS steadfastly refused to participate in such meetings until 2005, based on legal advice.

Eventually, the victims' families launched civil suits seeking damages. The government lawyers who were instructed to resist the families' claims were sent to the Coroner's Inquest in Ireland and to the Kirpal Inquiry in India. The Government instructed those lawyers to ensure that evidence about Canada was presented in the best light possible. Government counsel argued that there was no conclusive evidence that a bomb had caused the Air India crash, even while the RCMP was conducting a criminal investigation based entirely on the premise that the crash had been caused by a bomb and was gathering strong circumstantial evidence to support that premise.

The Government's position was that no finding could be made that Canadian security measures were inadequate. Underlying the position was an apprehension that a finding that Canada was blameworthy would bring about unavoidable political and financial costs, including an obligation to compensate the families, something the Government was fiercely determined to avoid. A decision was made to avoid filing a Canadian Aviation Safety Board (CASB) report that concluded that the crash had been caused by an explosion, not because the report was inaccurate, but because it implied that there may have been security failures at Canadian airports and because it linked the Air India and Narita bombings in a manner that would inevitably point to Canada as the location where the bomb was put on board the aircraft.

Defending the civil lawsuits was a matter of the highest priority to government agencies. CSIS finally stopped erasing the tapes for its intercept of Parmar's communications – not because of the criminal investigation, but at the express direction of the Department of Justice some nine months after the bombing – for purposes of civil litigation.

Media reports and their potential impact on the public image of the agencies also played a surprising role in the investigation. The RCMP only began actively to pursue certain aspects of its investigation in response to critical media reports or to deal with public relations concerns. The RCMP followed up on the November 1984 Bomb Plot information after allegations appeared in the media that the Force had been warned about the Air India bombing and had failed to act. The RCMP effort in 1995 to resolve all outstanding investigative issues was made with an eye to the ten-year anniversary of the bombing and with the purpose of being able to make a pre-emptive public statement, "…rather than reacting to media queries afterwards."[2]

The CSIS Director attempted to defend and justify the erasure of the Parmar tapes in a television interview, even while the BC Crown prosecutor was still waiting for answers from CSIS in this respect. In subsequent discussions, CSIS insisted that the erasure not be referred to as "destruction of evidence," in light of concerns about its reputation and potential civil liability.

---

2 Exhibit P-101 CAF0391, pp. 1-2.

Resistance to Review

When the Security Intelligence Review Committee (SIRC) first attempted to conduct a review of CSIS's activities in connection with the Air India bombing in the late 1980's, government agencies united in successful opposition to the review, citing possible interference with the ongoing criminal investigation and the prosecution of Inderjit Singh Reyat. The government agencies were reluctant to invest resources to shed light on deficiencies in their response. They also cited a concern that a review could negatively affect the Government's position in the civil litigation, fearing that negative conclusions could be used against them and that the release of information unhelpful to the Government's case would mean the lawsuit would become more costly to the Government.

By the spring of 1991, Reyat had been convicted for his role in the Narita bombing, and calls for a public inquiry were once again mounting. The agencies again took an aggressive approach in their attempts to stave off external review. An Interdepartmental Working Group formed by the Solicitor General's office prescribed a common front against a possible SIRC review on the basis of potential damage to the ongoing RCMP investigation, even though the ongoing RCMP initiatives were limited to wreckage recovery. When the review finally did proceed, the RCMP consciously limited the amount of information provided to SIRC and avoided any criticism of CSIS. The RCMP justified its approach on the basis of its desire to protect the ongoing investigation, then in its sixth unsuccessful year.

The opposition to external review did not end with SIRC. When it appeared that the RCMP investigation had reached an impasse in 1995, the Government considered whether or not to call a public inquiry. Rather than admitting in public that its investigation was at an impasse, the RCMP asked Gary Bass to review the Air India file. As a result, a renewed investment in the investigation was made. Commendable as the re-investigation may have been, it is unfortunate that it was the spectre of a public inquiry that motivated this long-overdue development.

The need to protect the "ongoing investigation" has continuously been invoked by the RCMP to justify insulating its actions from review and to prevent public disclosure of information by external reviewers, including the Commission. In its aggressive invocation of the precept of police independence and in its accompanying warnings about the potential to harm ongoing investigations, the RCMP at times has been, in the words of current RCMP Commissioner William Elliott, "…more standoffish than independent and our standoffishness has not worked to our advantage."[3]

Once the review by the Honourable Bob Rae was announced in 2005, the RCMP and CSIS attempted to demonstrate that initiatives were now in place to address long-standing issues, including cooperation problems. Many of these issues had been left unaddressed since 1985. It is as if the prospect of an external,

3 Testimony of William Elliott, vol. 90, December 6, 2007, pp. 11822-11823.

independent review moved the agencies to 'fix' problems so as to avoid the imposition of measures that would not be of their own choosing.

3.12.2 The Government's Voice

Throughout the post bombing period the Government has attempted to "speak with one voice", and thereby to avoid situations where its agencies would air their disputes and debates in public or reveal information that might lead to public criticism.

Counsel appointed to defend the civil litigation presented a unified position on behalf of Canada at the Coroner's Inquest and at the Kirpal Inquiry. In dealing with the SIRC review, the Air India Working Group took on the role of coordinating all Government agencies' briefings, with a mandate to ensure that the Government would present a consistent version of the facts, even at the expense of completeness and comprehensiveness. The RCMP briefing to SIRC took a particularly positive spin, with little or no criticism of CSIS and an emphasis on the good interagency working relationship. This position was in stark contrast with internal RCMP correspondence that emphasized failures in cooperation and was replete with criticism of CSIS.

Not surprisingly, SIRC took away from this briefing the view that issues of cooperation between CSIS and the RCMP had not had a significant impact on the RCMP investigation. The RCMP did not intervene to qualify or correct this perception, and chose not to comment on the SIRC report when it was released. The RCMP would come to regret these decisions years later and to view the findings in the SIRC report as potentially compromising the eventual prosecution of Malik and Bagri.

In the briefing it provided to Rae in 2005, the RCMP adopted an entirely different approach. Without Government-wide coordination, the briefing was more detailed (though unfortunately not always entirely accurate) and more critical. It even called into question the very SIRC findings that were based on the RCMP's briefing to SIRC. The RCMP provided a detailed list of its grievances about the behaviour of CSIS. CSIS responded in kind by noting that some information in the RCMP submission was "simply incorrect."

External review should be an opportunity for the institutions to reflect on possible past mistakes and on the measures that might be implemented to avoid repeating them. It should not be seen as an opportunity to head off changes that might be suggested by the reviewer. Nevertheless, the agencies' positions in their briefings to Rae, with all their defensiveness and finger-pointing, had at least the merit of constituting a more genuine representation of their respective institutional views, as opposed to the Government's "one voice".

3.12.3 That Was Then, This Is Now

The strategy adopted for two decades by CSIS and the RCMP when responding to external review has generally been to argue that any problems in interagency

cooperation that may have arisen in the past had since been resolved through initiatives that had been implemented to improve cooperation.
As revealed by the RCMP's submissions to Rae, the message of "that was then, this is now" was never particularly accurate, despite its repeated invocation. The RCMP explicitly admitted that many of the challenges faced in 1985 still remained in 2005, despite the earlier messages, including that given to SIRC in 1992, that all cooperation problems were resolved.

CSIS, on the other hand, did not refer to any ongoing problems in the current relationship in its briefing to Rae, and continued instead to point to the progress that had been made in the relationship and the fact the agencies were now working closely together.

3.12.4 The Present Inquiry

The Prime Minister called this Inquiry to request answers to seven difficult policy questions relating to the past and present practices of government agencies in relation to the Air India matter and to terrorism and aviation security more generally. The Inquiry was also meant to provide long-awaited answers to the families of the victims. The approach of the government agencies to this Inquiry has, in many ways, followed the pattern of reticence and defensiveness they adopted throughout the post bombing period.

Although a public inquiry sometimes looks like a trial, with examinations and cross-examinations conducted by lawyers, it is essentially quite different. Its purpose is not to find liability, but rather to get at the truth and to learn from past mistakes. As its name suggests, it is an examination (or, to use a word with negative connotations in the English language) it is an "inquisitorial" process rather than an adversarial one.

Since it is the Government that calls the Inquiry and sets its mandate, the Government's ultimate interest lies in having the Inquiry succeed in getting at the truth in order to allow it to make useful recommendations intended to resolve problems and to avoid the repetition of past mistakes. For that endeavour to succeed, and for the Inquiry to reach its goals, it is crucial that Government be as forthcoming, transparent and candid as possible in providing information.

The course of this Inquiry has demonstrated that old habits sometimes die hard. The same defensiveness and reflexive secretiveness that the Commission noted in the attitude of the government agencies in dealing with the aftermath of the bombing were at times evident during the course of this Inquiry.

Each of CSIS, the RCMP and Transport Canada have valid interests in preventing disclosure of any information that would threaten national security, ongoing criminal investigations and the security arrangements at Canada's airports. Those legitimate concerns made it inevitable that relevant documents and information held by Government would need to be reviewed and, where necessary, "redacted" (i.e. censored) prior to public disclosure so as to protect

these interests. In practice, however, the approach to redaction taken by the agencies proved to be overly broad and seemingly based on a mechanical application of a set of abstract rules with little, if any, attention paid to any actual harm that might ensue from disclosing information that was more than two decades old.

The initial position taken by the agencies resulted in hundreds of documents being largely, or even entirely, blacked out. The Government took extensive objection to the public disclosure of information, to the point where no meaningful public examination would have been possible. It was only after the direct and welcome intervention of the Prime Minister that these positions were reconsidered and it became clear that most of the information that was originally sought to be suppressed was capable of being disclosed with no risk to Canada's actual security or to its legal interests. This exemplified former RCMP Commissioner Zaccardelli's observation that federal agencies tend to "… over-classify… over-redact and then… ultimately get embarrassed by it being shown not to have been necessary so many times."[4]

While matters improved to the point where it became possible to hold public hearings after the Prime Minister's intervention, problems persisted.

In his evidence, former SIRC Chair Ronald ("Ron") Atkey noted that, in his experience, "CSIS were very good at responding to your questions, but only to your questions."[5] The Commission experienced a number of examples of this reticence, which, when combined with continuing examples of overly aggressive claims for National Security Confidentiality, made telling the CSIS story more difficult than was necessary.

Transport Canada was undoubtedly justified in trying to prevent unnecessary disclosure of security details related to airports and aviation, but it did not always exercise appropriate restraint, particularly with regard to historical information of key importance to the Commission's Terms of Reference. Its unfounded claims of privilege regarding certain information not only unnecessarily delayed public disclosure, but also limited public debate and discussion of clearly relevant matters. The Government position was reminiscent of the Government-wide two decade long preoccupation with avoiding any potential admissions of error or of substandard performance in the destruction of Flight 182.

Most troubling, however, was the RCMP's reliance on the notion of the possible effects on the "ongoing investigation". The spectre of this danger was used in ways that were occasionally inappropriate and that had the potential to interfere with the work of the Commission.

In January 2007, the RCMP was contacted by an individual, Mr. G, who was an important figure in the Sikh extremist movement in 1985 and who was believed

4 Testimony of Giuliano Zaccardelli, vol. 86, November 30, 2007, p. 11082.
5 Testimony of Ronald Atkey, vol. 49, September 20, 2007, p. 5969.

to have knowledge about the Air India bombing. Mr. G wanted to testify in this Inquiry. Without advising the Commission about Mr. G's approach, the RCMP made the unilateral decision, that its "revived" investigative interest in Mr. G should have priority over the work of the Commission and that it should have the first and exclusive opportunity to investigate any information Mr. G might have. The RCMP proceeded to request additional redactions to the material that was to be entered into evidence about Mr. G, telling the Commission that Mr. G had recently demonstrated a newfound willingness to cooperate, and that the redactions were necessary to protect this "new initiative" in the ongoing investigation. The RCMP did not advise that Mr. G wanted to speak to the Commission.

The last time the RCMP had spoken to Mr. G before this Inquiry was in 2000. At that time, Mr. G had provided information, but the prosecution decided not to call him as a witness in light of the contradictions in his past statements. The RCMP always believed that Mr. G knew more, but for the past seven years had done nothing to pursue him.

Despite Mr. G's repeated requests to testify before the Commission throughout the following months, the RCMP did not advise the Commission. Instead the RCMP asked Mr. G to delay his plan to contact the Commission. During a formal interview with the RCMP in September 2007, Mr. G complained that he had not been able to contact the Commission. RCMP investigators told him that he could contact the Commission if he so wished, but that Commission staff "were not investigators" and that they would simply refer him back to the RCMP.

The RCMP had not been successful in the past in obtaining from Mr. G the additional information the Force believed he possessed and it was no more successful in 2007. Nevertheless, even after it had dropped its pursuit of Mr. G's information, the RCMP still did not advise the Commission of Mr. G's interest in testifying at the inquiry, nor did it take steps to allow lifting of the additional redactions it had sought on the basis of this new "ongoing investigation" initiative. It was only by accident that the Commission discovered that Mr. G was potentially interested in testifying. It was not until March 2008, months after the Commission had specifically asked whether Mr. G had expressed any interest in speaking with representatives of the Inquiry, that the RCMP finally advised the Commission, a month after the hearings were concluded, that Mr. G "…was at one point prepared to speak with representatives of the Commission."

All these lapses by the various agencies seem to the Commission to have been unnecessary and to have been the product of years of habit rather than of any intent to interfere with the work of the Inquiry. Taken together, they seem to fall in line with the defensiveness and reluctance to acknowledge error that characterized the reflexive and un-reflective responses of these agencies throughout the post bombing period.

It is notable that, perhaps because of this default defensiveness, no one who testified on behalf of any of the agencies of government thought it appropriate

to apologize to the families of the victims for the errors and omissions of the Government and its agencies or for the treatment to which the families have been subjected by the Government as a result of its apparent determination to avoid an obligation to provide them with meaningful compensation.

It is telling that the only Government witness who expressed regret about the quality of the information that had been provided to the families was a former CSE (and current CSIS) employee, who asserted bluntly that the families had been misled by Bartleman's testimony and by his implicit criticism of the Government's pre-bombing conduct. Interestingly, the witness also insisted that he would not feel responsible for the families' plight, based on what turned out to be his inaccurate conclusion that no CSE intelligence existed that could have forewarned of the bombing or led to a different security response.

While this particular incident stands out as a rather astonishing and extreme example of denying the negative, in general, government witnesses seemed nearly unanimous in emphasizing the positive in their testimony. With the exception of the thoughtful and balanced testimonies of former CSIS DG CT James ("Jim") Warren, of former High Commissioner to India William Warden, and of former RCMP Staff Sergeant Robert Solvason, government witnesses seemed loath to acknowledge that any errors at all had been made or that there were any deficiencies in performance by government agencies. This sunny attitude spilled over into the submissions of the Attorney General of Canada, through which the Government of Canada and all its agencies spoke with one voice during the Inquiry.

Notwithstanding the fact that the Government called this Inquiry, asking for recommendations to solve problems and deficiencies, and to prevent the recurrence of past problems, the final position presented on behalf of Government is that, without admitting that there were any serious deficiencies in the past, whatever problems there might have been are all in the past. That was then; this is now, and no significant change to legislation policy or practice is necessary or advisable.

The Commission disagrees. Errors were made. Each of the relevant agencies of government showed clear deficiencies in performance that were often related to, or accompanied by, deficiencies in policy and in the understanding or application of legislation.

Volume Three chronicles in detail some of the deficiencies in performance. Volumes Three and Four deal with specific recommendations to address a number of the systemic, regulatory and legislative deficiencies.

VOLUME ONE
THE OVERVIEW

CHAPTER IV: INTELLIGENCE AND EVIDENCE

4.0 Introduction

Terrorism is both a serious security threat and a serious crime. Secret intelligence collected by Canadian and foreign intelligence agencies can warn the Government about terrorist threats and help prevent terrorist acts. Intelligence can also serve as evidence for prosecuting terrorism offences.

Volume Three addresses the issues that arise from using intelligence as evidence in criminal investigations and trials. Using intelligence as evidence can create a tension between the secrecy essential for the operations of the intelligence community and the openness demanded by the criminal trial process. Volume Three recommends having the National Security Advisor resolve this tension, acting in the public interest instead of in the sometimes narrower interests of the agencies involved.

The delicate balance between openness and secrecy presents challenges at each stage of the response to the threat of terrorism. Each terrorist threat is unique, and will require a response tailored to the specific circumstances of the threat, so it follows that there can be no presumptively "best" response. In some cases, it will clearly be appropriate to engage the police early on. In others, it may better serve the public interest to allow intelligence agencies to continue to monitor and report on the threat or to use other, non-police, agencies to disrupt an evolving plot. The most effective use of intelligence may not even involve the criminal justice system.

Canadian efforts against terrorism involve many entities, including the Canadian Security Intelligence Service (CSIS), the Canada Revenue Agency (CRA), the Royal Canadian Mounted Police (RCMP), the Department of Foreign Affairs and International Trade (DFAIT), the Canada Border Services Agency (CBSA) and the Communications Security Establishment (CSE). Each agency has its own mandate and rules governing how it carries out that mandate. The mandates sometimes overlap.

4.1 Secrecy vs. Openness

Even with the best intentions, coordination and effective communication among the many agencies involved in the counterterrorism effort in Canada can be very difficult.

Both the pre-bombing and post-bombing phases of the Air India tragedy demonstrate the challenges that these agencies experienced in communicating effectively with each other and in respecting each others' rules and requirements while, at the same time, looking out for their own institutional interests.

During the pre-bombing phase, CSIS did not get important information from other agencies, including CSE and the RCMP, and hence was unable to provide a meaningful assessment of the threat to Air India flights. In the post-bombing phase, CSIS collected and dispersed information according to its own rules and intelligence requirements, but in the process made the information unavailable to or unusable by the criminal justice system. This impaired the quality of the evidence available to the prosecution and compromised the fair trial rights of the accused. When CSIS passed information to the RCMP, the RCMP was often careless in respecting caveats or in appropriately protecting sources and methods. As for the criminal justice system, its focus on complete and wide-ranging disclosure repeatedly encountered resistance in the form of the intelligence community's basic imperative to protect the confidentiality of its sources, methods and information.

While CSIS faces potentially adverse consequences as a result of sharing information with the police, there are no similar consequences for other agencies that share information with CSIS. There is no excuse for any agency failing to share information with CSIS. Security-related threat information collected by the RCMP for law enforcement purposes can, and ought to be, shared with CSIS in all but the rarest of circumstances. The Commission does not view the report or recommendations of the O'Connor Commission as being in any way inconsistent with this observation.

Agencies must share information with each other to respond effectively to terrorist threats. However, Canadian agencies have developed a culture of managing information in a manner designed to protect their individual institutional interests. This approach compromises coordination and effective communication among agencies.

The decision of an intelligence agency to share intelligence with the police may have far-reaching implications for ongoing intelligence investigations, for the agency's sources and for the targets of investigations. The governing imperative for intelligence-gathering agencies is to preserve tight restrictions on the dissemination of information. This imperative makes sense, for several reasons. First, collecting intelligence is largely a clandestine activity. Foreign governments and intelligence services restrict, often explicitly, the further disclosure of their intelligence as a condition of sharing it with CSIS. Valuable intelligence often comes from sources who cannot be revealed publicly without jeopardizing their continuing usefulness and, possibly, their safety. Almost always, intelligence agencies prohibit the dissemination of information beyond CSIS, seriously impeding law enforcement. This is a reality of the modern security intelligence environment.

Second, intelligence agencies resist public disclosure of information due to the realistic fear of compromising the investigation for which it has been collected. Public disclosure, or even limited disclosure to law enforcement, can interfere with sensitive intelligence investigations and even lead to their termination. Compromised investigations may harm Canada's international strategic interests and threaten the safety of individuals involved in gathering intelligence.

A further plausible reason for CSIS resisting disclosure is rooted in the intrusive means by which it is authorized to collect intelligence. The basis for a *Criminal Code* warrant application is that the affiant has reasonable grounds to believe that an offence has been, or will be, committed. An affiant applying for a section 21 warrant under the *CSIS Act* must only have a belief, on reasonable grounds, that a warrant is required to enable CSIS to investigate a threat to the security of Canada. The affiant does not need to specify a reasonable belief that an offence has been, or will be, committed. The section 21 warrant could relate to someone reasonably suspected of being involved in a terrorist or other threat to the security of Canada, even if no offence is specified. For this reason, it is likely that a CSIS warrant will be less difficult to obtain than a *Criminal Code* warrant in the early stages of a terrorist conspiracy or plot. Easy disclosure to the police of material collected under a CSIS warrant could risk, in the words of Geoffrey O'Brian, one of the first civilian employees of CSIS, turning CSIS into a "cheap cop shop."

These reasons explain and, in some measure, justify resistance by CSIS to public disclosure of intelligence. However, there are situations in which the disclosure of intelligence by CSIS to law enforcement is in the public interest.

From the point of view of the criminal justice system, the ruling imperative is the public production of as much potentially relevant information as possible. The right to a fair trial, entrenched in section 7 of the *Charter*, requires that all relevant information in the possession of the prosecution be given to the accused person, no matter whether it tends to support or to undermine the case for the prosecution. In our open system of justice, the information upon which guilt or innocence is determined must be made public. To justify the serious sanctions that can be imposed by the criminal justice system, the system requires reliable proof to a very high standard. These requirements cannot be circumvented or compromised. As a result, the compelling reasons for the intelligence community to maintain secrecy are balanced by equally compelling reasons for the criminal justice system to require openness. Effective protection of national security depends on both the intelligence-gathering system and the criminal justice system. Effective cooperation among agencies in sharing and using intelligence is not merely a subject of theoretical debate; it is a practical necessity.

4.2 Concurrent National Security Mandates and Information Sharing

The counterterrorism mandates of CSIS and the RCMP overlap to a significant degree. The consequences of a terrorist threat fall squarely within the core mandate of CSIS, which is to advise the Government of Canada on the nature and extent of threats to national security. As a criminal offence, terrorism is equally central to the RCMP mandate to investigate and prosecute serious crimes. The extent of the overlap is highlighted by the 2001 *Anti-terrorism Act* definition of the criminal offence of "terrorism." Terrorism extends both to completed acts of violence and to the planning and providing of assistance for such acts, whether or not they have come to fruition. CSIS and the RCMP are each legitimately involved in investigating the same activities.

Developments in criminal jurisprudence have put pressure on CSIS to make intelligence public in the criminal process. The Supreme Court of Canada decision in *R v. Stinchcombe* clarified beyond all debate that the prosecution has an obligation to disclose all potentially relevant material in its possession to the accused. At around the same time as the *Stinchcombe* decision, courts began looking behind claims of "national security confidentiality," testing the accuracy of the affidavits used to justify search warrants and wiretap applications, before admitting material gathered on the basis of such warrants into evidence at trial. These developments set the CSIS imperative of secrecy directly into conflict with the criminal justice system's requirement to disclose all potentially relevant information to the defence.

Because CSIS will usually begin the investigation of a threat well before there is any element of criminality, it will have much more information than will the RCMP. Once engaged in the investigation, however, the RCMP will want as much information from CSIS as it can get. CSIS information might be vital in that it may help the RCMP to understand the threat and to fill in any gaps in the body of information in its case.

For reasons already discussed, CSIS may be cautious about disclosing – and may even be categorically unwilling to disclose – information to the RCMP without a guarantee that the information will not be made public. Understandably, the RCMP cannot make such an assurance. If its own investigation leads to a prosecution, the RCMP will be required to disclose all potentially relevant information to the Crown and, eventually, that information will be disclosed to the defence and perhaps made public in court. Because of this, CSIS might try to avoid providing the information to the RCMP to protect the viability of its ongoing investigation.

These opposing interests over the use of CSIS intelligence can, in the extreme, lead to the unpalatable choice known as "disclose or dismiss": either disclose relevant information to the defence, even if it may contain sensitive intelligence, or protect the information, but risk failure to proceed with a case against an accused terrorist.

The "disclose or dismiss" dilemma has arisen in terrorism prosecutions both before and after *Stinchcombe*. This has resulted in the termination of several prosecutions before verdicts were reached. Notably, two of these have involved allegations of Sikh extremism. In one of the two, Talwinder Singh Parmar was the accused.

Paradoxically, the risk to criminal cases presented by the desire to protect sensitive intelligence has motivated the RCMP to avoid acquiring information from CSIS.

As discussed in detail in Volume Three, there are numerous ways to avoid the conflict between the desire to keep intelligence secret and the obligation to disclose potentially relevant information in a criminal trial. However, the perception that a choice may have to be made results in both CSIS and the police looking for ways to keep the intelligence out of the hands of the police. No matter how unintentional, the result will be to impoverish the response to terrorist threats. Something has to change in the approach taken towards the transfer of intelligence to the hands of law enforcement.

4.3 Ineffective Responses to the Disclosure Dilemma

4.3.1 Informal Solutions

The evidence shows that both CSIS and the RCMP, though they both may regard the result as far from optimal, have concluded that the best management of the potential "disclose or dismiss" dilemma is to avoid the problem entirely by ensuring that the minimum of potentially disclosable intelligence is passed from CSIS to the RCMP.

This misguided strategy is not new to either agency. From its inception, the "civilianization" of CSIS led it to adopt the mantra that "CSIS does not collect evidence." CSIS policies had the effect of rendering most CSIS information unusable in court and of limited value to the police. There may have been no nefarious purpose behind these policies. They accorded with the overwhelming sentiment at that time that a clean line needed to be drawn between CSIS as a civilian intelligence service and the RCMP as a law enforcement agency.

The consequences of the erasure of the Parmar tapes demonstrated that the policies regarding the collection and storage of information adhered to in order to protect CSIS information from disclosure in court did not in fact make CSIS intelligence irrelevant or immune from disclosure. The information on the destroyed tapes might have been of no use to either the prosecution or the defence in the Air India trial, and it might have been inadmissible at the trial based on a number of principles under the law of evidence. Still, the destruction of the tapes prevented the prosecution from disclosing their contents to the accused. This led to the worst possible results for CSIS and for the prosecution. The tapes were ruled disclosable and their destruction was held to be an abuse of process.

The larger lesson from this episode, one that may not be fully understood as yet by CSIS or the RCMP, is that efforts to keep potentially relevant CSIS information out of the hands of the RCMP are not effective. Disclosure obligations are engaged by the potential relevance of the information, not by its evidentiary status or by who holds it. It is for this reason that the philosophy of "the less information we receive from CSIS, the better" (curiously described in testimony as a "less is more" philosophy), adopted by the RCMP, is equally unlikely to shield CSIS intelligence from disclosure or to protect prosecutions in which the information is not disclosed.

The philosophy of "the less information we receive from CSIS, the better" is based on an assumption that the obligation to disclose would apply only to material that is in the hands of the RCMP; if CSIS did not provide material to the RCMP, the material would be deemed not to be in the Crown's possession and there would be no obligation to disclose that material to the defence.

The fact is that relevance, not custody, determines what the prosecution must disclose to the defence. There may be a privilege or legally recognized right that a person or institution may raise to persuade a court that, despite relevance, the material ought not to be disclosed. However, it is not possible to avoid the obligation to disclose simply by withholding the information from the police in the first place. Accordingly, the prosecution should pursue all relevant material, particularly if the information is in the hands of government entities that have investigated the matter now before the trial court.

The real possibility of the accused obtaining disclosure of intelligence from CSIS suggests that the RCMP approach of avoiding the acquisition of intelligence from CSIS is not an effective or reliable means of protecting that intelligence from disclosure. It also deprives the RCMP of valuable information. Hence, the philosophy of "the less information we receive from CSIS, the better" should be abandoned. A better approach, whenever possible, is for CSIS to collect intelligence in counterterrorism investigations with the expectation that it may be disclosed or used as evidence in court.

4.3.2 Proposed Legislative Changes

From time to time, both CSIS and the RCMP have proposed that information-sharing challenges might be resolved through legislation. In general terms, these proposals range from the removal of legislative barriers to the flow of information from CSIS to the RCMP to the creation of legislative limits on the information that the criminal justice system can demand from CSIS. Each of these proposals addresses only one aspect of the problem, and thus will ultimately be ineffective in serving the public interest.

The Attorney General of Canada (AGC) can apply to the Federal Court to prevent disclosure of sensitive national security information by invoking section 38 of the *Canada Evidence Act*. Where disclosure for purposes of criminal proceedings is involved, the Federal Court examines whether the material could cause harm

to Canada's national security or international relations. If the answer is "no," the Court will refuse to bar disclosure. If the answer is "yes," the Court will consider whether failure to disclose will harm the fair trial rights of the accused person. If the answer to this second question is "no," the Court will bar disclosure outright. If the answer is "yes," the Court will still bar disclosure, but can consider a range of possible remedies, including releasing edited documents or providing unclassified summaries of the documents or information in question in order to mitigate the effect of barring direct disclosure.

This process allows CSIS to protect sensitive intelligence information, but both CSIS and the RCMP see the process as having several significant drawbacks. The outcome is inherently uncertain. Neither CSIS nor the RCMP can know at the beginning of the process – the point of disclosure by CSIS to the RCMP – what its conclusion will be.

Furthermore, the process for determining whether sensitive intelligence information can be withheld does not end with the Federal Court's determination of the section 38 application, or even with the conclusion of any appeals to the Federal Court of Appeal and Supreme Court of Canada. Whatever the ruling by the Federal Court, the Attorney General of Canada still has jurisdiction to order disclosure or to prohibit disclosure of any information or document. All this clearly adds to the uncertainty for CSIS, and also introduces uncertainty for the RCMP and, ultimately, for the prosecution.

It is, therefore, not surprising that, at the extreme end of the spectrum, proposals have been put forth for a legislated privilege which would remove any national security material from the criminal justice system. Intelligence would not need to be disclosed to the accused in the same way that the identity of a police informer is not disclosed.

In a post-*Charter*, post-*Stinchcombe* world, it is not possible simply to ignore the right of an accused person to a fair trial, a right that includes disclosure of all relevant information capable of assisting an accused person in making "full answer and defence" to the charges. No blanket privilege can trump these *Charter* rights. Even the police informer privilege, perhaps as bullet-proof a privilege as can exist in the criminal law sphere, cannot prevail when "innocence is at stake."

To ensure that a "national security privilege" would comply with the *Charter*, it would be necessary to qualify the privilege by requiring disclosure to the extent necessary to ensure a fair trial. This would produce the same situation as when the trial judge considers whether any orders under section 38 infringe an accused person's right to a fair trial. The intelligence information might not need to be disclosed, but if it were not disclosed, the case against the accused might have to be dismissed.

A different proposal to limit the flow of information in the disclosure process involves the suggestion that the disclosure requirements set out in *Stinchcombe* should be limited by statute. This is a suggestion often made by the police,

who bear the brunt of the *Stinchcombe* disclosure requirements, which are sometimes described as the most onerous of any Western democracy. However, insofar as the problem of excessive resources devoted to needless disclosure applies to the criminal justice system in general, one should be cautious about identifying this problem as residing in the *Stinchcombe* test itself.

The constitutional dimension of *Stinchcombe* consists of a right to all relevant information touching on the accused's ability to defend him- or herself. In order to make such disclosure, someone must go through the raw material to identify all potentially relevant information and then identify that which is actually relevant. This will require separating the clearly irrelevant from the possibly relevant (which is another way of saying "not clearly irrelevant") and, then, the actually relevant from the possibly relevant.

However, this is not to say that practical and cost-saving measures in relation to *Stinchcombe* disclosure obligations cannot be taken. Volume Three proposes that, in terrorism prosecutions, the Crown should be permitted to provide in electronic form any material on which it intends to rely and should have the discretion to provide paper copies of such material. Material on which the Crown does not intend to rely, but which is relevant, should be produced in electronic format. The Crown should be able to disclose all other material that must be disclosed pursuant to *Stinchcombe* and the 2008 decision in *Charkaoui* by making it available to the accused for manual inspection.

In any event, whether the rules for initial disclosure obligations are broadly or narrowly articulated, the fundamental constitutional obligation is always the same: for a fair trial, the defence must have disclosure of all material necessary to make "full answer and defence."

On the other end of the spectrum are proposals designed to enhance the sharing of intelligence with police. Volume Three discusses an amendment to section 19(2) of the *CSIS Act* to remove the current CSIS discretion concerning whether or not to disclose information to police. However, solutions of this nature are paradoxically likely to do both less and more than one might expect.

On the one hand, requiring disclosure is not tantamount to ensuring that the information will be admissible at trial. There would still be an opportunity for CSIS to object to public disclosure at trial on national security grounds under section 38 of the *Canadian Evidence Act*, and thus potential "disclose or dismiss" situations would not be avoided.

On the other hand, mandatory disclosure would have the unsatisfactory result of giving the RCMP the power to decide unilaterally what should be done with sensitive CSIS information.

The problem is that allowing the needs of the criminal justice system to take priority over other considerations will not always be in the best interests of

Canada. There may be good reasons for CSIS to avoid passing information to the RCMP. Leaving the choice of whether and when to commence a criminal investigation to the RCMP is unlikely to lead to better decision-making.

Any workable legislative changes cannot be based upon an a *priori* view that favours one of either law enforcement or the intelligence community over the other. Instead of approaching these issues from the perspective of individual agency concerns, the solution lies in making changes that allow for the public interest to be identified and acted upon.

4.4 Towards the Effective Management of the "Intelligence into Evidence" Problem

No "silver bullet" can exempt relevant intelligence from disclosure without consequences for the viability of a criminal prosecution. Once the intelligence and law enforcement communities accept that reality, they can focus on realistic and pragmatic practices and procedures that can minimize the potential for adverse consequences caused by using intelligence in criminal prosecutions.
First and foremost, the goal of such an approach should be to establish means to avoid a stark choice between the needs of a fair trial and those of national security. A realistic and pragmatic approach by the intelligence community would be to recognize that, as long as the criminal justice system remains an important means by which Canada seeks to deal with terrorism, intelligence may be relevant to the criminal justice system from the moment a terrorist conspiracy begins to unfold.

For that reason, it is necessary for the intelligence community to abandon the notion that "CSIS does not collect evidence" as a justification for practices that compromise the use of CSIS information in ensuing criminal investigations or prosecutions. The duty of disclosure of relevant information is entirely separate and distinct from the issue of whether the means by which the information was gathered, preserved and stored make it admissible as evidence at trial. CSIS has nothing to lose by ensuring that its practices in gathering, retaining and sharing information do not compromise the potential admissibility of the information as evidence in a criminal trial.

So long as the information is relevant, it will have to be disclosed, subject to national security privilege. On the other hand, a failure to follow such procedures can profoundly and, in some cases, irremediably, harm the interests of the justice system by making it more difficult to combat terrorism. Failure to provide prosecutors with usable information can compromise the viability of terrorism prosecutions to the extent that the ability to provide a fair trial to accused persons may be impaired, as illustrated by Justice Josephson's ruling on the erasure of the Parmar tapes in the Malik and Bagri trial.

In response to the Supreme Court of Canada's 2008 decision in *Charkaoui*, CSIS may now be attempting to reform its internal procedures for the retention

of information to comply with the Court's observations about CSIS retention obligations. As it approaches this task, CSIS should adopt procedures and provide training that will ensure that the methods by which information is retained and stored are capable of serving the interests of both the intelligence and law enforcement communities. This should include procedures for retention of the original materials (documents, interview notes, audio or video recordings) as well as practices to ensure demonstrable continuity of possession. It would be useful for the Service to seek the advice of the RCMP and the Department of Justice on the best approach to this.

Self-restraint and self-discipline in and by the institutions involved in the intelligence community and the criminal justice system would serve them well in combatting this problem. It is time for each institution, and the actors within it, to adopt a broader perspective and to avoid patterns of behaviour that may serve narrow institutional interests well but the public interest poorly.

For the intelligence community, this means not overstating the need for secrecy. For defence counsel, it means avoiding burdening the court with frivolous pre-trial applications. For prosecutors, it means avoiding "overcharging." For judges, it means becoming less tolerant of tactics used by counsel to try, for partisan advantage, to bring national security interests into conflict with the right to a fair trial. These issues, as well as the sheer volume of disclosure, can make the trial process cumbersome and, seemingly, out of control.

Defence counsel should abandon frivolous pre-trial applications, which lengthen proceedings, making criminal trials a war of attrition. A mature attitude and increased cooperation among counsel are needed. Many pre-trial applications can be avoided by using agreed statements of facts. Much of the "bulk" of a criminal trial can also be reduced by agreed statements of fact and admissions of matters not in dispute, allowing the judge to focus on what is truly in dispute.

Prosecutors should lay charges only for acts that they can prove. Prosecutors should not lay every possible charge against as many accused as possible. These "loaded indictments" unduly complicate criminal proceedings and bog them down in lengthy procedural wrangling.

Trial judges bear a significant responsibility. They are ultimately in charge of their courtroom and of the trial process. Too often they are timid and unwilling to rein in wayward counsel. Trial judges must make greater efforts to keep trials on track and focused on relevant matters. They need to develop a relationship with counsel so that all appreciate the need to cooperate.

None of this is intended to diminish the adversarial process. Rather, it is meant to focus the criminal trial on what is truly at issue and requires a determination to do so, be it about alleged breaches of the *Charter* or about an essential element of a criminal charge.

Volume Three contains a detailed discussion of possible procedural changes that may better enable the criminal justice system to cope with the unique challenges of terrorism prosecutions. The Commission gave careful consideration to suggestions for changes, including those from the Air India Victims Families Association. The terms of reference required the Commission to examine whether there is merit in having terrorism cases heard by a three-judge panel. The panel could replace a judge sitting alone or a judge and jury. While the Commission understands the thinking behind considering this mode of trial, it has concluded that the resulting procedural and legal complexities would make three-judge panels impractical and inadvisable.

4.5 Reforming Decision-Making

Even with the best efforts of the institutions involved in national security and criminal justice issues, their competing interests in the "intelligence-evidence" debate cannot easily be reconciled. An effective means of resolving these conflicts is necessary.

At several key times, choices may need to be made between the legitimate interests of the intelligence community and those of the criminal justice system. For each of those times, effective resolution will depend on the continual improvement of the decision-making process rather than on any formula for weighing the importance or the legitimacy of the competing interests. Former Commissioner Zaccardelli astutely observed that such decisions need to be made "in the interests of Canada." To resolve differences between competing interests in a manner that places the broader public interest above the narrower concerns of any agencies involved, the decision-maker must be sufficiently independent of the conflicting agencies.

4.5.1 The National Security Advisor

The first major point at which the interests of the intelligence community may diverge from those of the criminal justice system occurs when CSIS decides whether it should disclose information to a police agency about a possible terrorism offence.

CSIS and the RCMP share the reasonable expectation that the criminal justice system will be a vital tool for responding to planned terrorist acts. The police will investigate such plans, the Crown will prosecute and the courts will adjudicate. Testimony heard by the Commission suggests that CSIS will usually have no objection to disclosing such information to the RCMP in most cases. As CSIS adopts procedures about the disclosure of the intelligence that it gathers for use in criminal proceedings, the percentage of cases in which CSIS voluntarily discloses intelligence to the RCMP will likely rise.

Nevertheless, the possibility of a police investigation and resulting criminal prosecution can mean that CSIS might lose control over the further disclosure of

its intelligence. In such an event, the identities of CSIS sources and employees, the secrets of its allies and the integrity of its long-term investigations may be jeopardized. For that reason, it seems inevitable that CSIS will sometimes be reluctant to pass intelligence to the police, or that it will decide to postpone such disclosure.

The *CSIS Act* gives CSIS discretion about whether and when to disclose intelligence to the police. It is neither reasonable nor efficient to put CSIS in the position of weighing its own interests against those of law enforcement and, possibly, expecting CSIS to decide against its own interests.

Disclosure decisions related to the implementation of the government's overall anti-terrorism strategy should be made by the National Security Advisor (NSA) to the Prime Minister. Because the NSA reports only to the Prime Minister, it is appropriate that the ultimate responsibility for deciding what Canada's national interest requires remain at the highest level of government. The NSA is intimately familiar with the needs and the interests of the intelligence community and, as a result, has a broad understanding of the overall national security landscape and the potential impact of the involvement of the criminal justice system.

The courts and the police must remain free from external direction. The police must be independent of government direction about when and what they investigate, for example. For this reason, NSA would not attempt to direct RCMP investigators. However, the NSA should decide if and when CSIS intelligence should be passed to the RCMP if CSIS initially is reluctant to do so. CSIS would then be required to pass the intelligence to the RCMP, which in turn would use the intelligence to decide whether a police investigation is warranted. The NSA would provide high level coordination of the anti-terrorism effort, while taking into account the interests of CSIS and the RCMP.

The NSA would require assistance in determining the possible effects of any of its decisions on CSIS, the police and on the criminal justice system. The NSA would need support in assessing the usefulness of passing the information to law enforcement agencies. The NSA should have secondees from the RCMP on staff. These secondees would be able to inform the NSA regarding which investigations the police are likely to pursue. The NSA will also need adequate legal expertise, especially to address disputes that may arise in the relationship between intelligence and evidence. To this end, personnel from the office of the proposed Director of Terrorism Prosecutions should, if needed, be seconded to the staff of the NSA.

The NSA should be someone who understands intelligence issues and who acts independently in helping to arbitrate differences of opinion between government agencies. It is not necessary that the NSA be recruited within government. A premium should be placed on finding an individual with sufficient stature and experience to command the respect of the intelligence community, while also having the Prime Minister's confidence.

4.5.2 Director of Terrorism Prosecutions

The Attorney General of Canada has delegated most decisions about laying or staying charges and about the general conduct of prosecutions by federal prosecutors to the Public Prosecution Service of Canada. The bulk of federal prosecutions occur largely in specialized areas of criminal and quasi-criminal proceedings, including drug offences, *Competition Act* violations and immigration matters. However, this is not the appropriate institution to conduct terrorism prosecutions.

Terrorism is an existential threat to Canadian society in a way that murder, assault, robbery and other crimes are not. Terrorists reject and challenge the very foundations of Canadian society.

In any criminal matter, prosecutors examine several factors when deciding whether to prosecute. These factors always include the public interest. In terrorism cases, however, determining the best course of action consistent with the public interest involves different considerations from those in most criminal cases. In terrorism cases, the public interest is the aggregate of considerations which includes national security, international relations and the impact of prosecutions on sensitive intelligence operations.

For this reason, decisions about proceeding with a terrorism prosecution should be made by the Attorney General of Canada. The AGC has the resources and the legitimacy to take into account the public interest in a way that a delegate does not. A quasi arm's-length agency like PPSC is, by design, independent from government and, as such, is unsuited to make determinations about the public interest where terrorism cases are involved.

There is also a need for expertise in terrorism prosecutions. It would be advisable to create a position of Director of Terrorism Prosecutions (DTP), serving under the Attorney General of Canada, to create a pool of experienced counsel for terrorism prosecutions. This small team of counsel could also provide legal advice about the conduct of national security confidentiality proceedings under section 38 of the *Canada Evidence Act* and give legal advice to agencies that collect intelligence and evidence in terrorism investigations.

The DTP should also be the decision-maker regarding the use of human intelligence sources as witnesses, as well as the liaison with police, intelligence services and foreign partners on matters concerning terrorism and national security.

The DTP should prosecute the criminal allegation and litigate all privilege claims, including those involving national security privilege. The DTP would work closely with the intelligence and law enforcement communities. This harmonized approach should promote carefully considered and fair terrorism prosecutions.

4.6 Determining National Security Privilege Claims

In a terrorism prosecution, the Attorney General of Canada may have to consider asking the Federal Court not to authorize the disclosure of information, in order to prevent harm to international relations, national defence or national security. If the Court agrees and refuses to authorize disclosure, the defence will be denied the information, but the prosecution will also be unable to rely on that information to secure a conviction. The legal basis for such a claim is found in section 38 of the *Canada Evidence Act*, and is known as national security privilege.

Two questions are central to the processes of litigating the section 38 claim and proceeding with the criminal trial. Would disclosure of the information harm Canada's interests? Is the disclosure of the information truly necessary for the defence to be able to respond to the charges?

The section 38 procedure requires two different courts to decide similar and closely related issues. Any non- or partial non-disclosure order made by the Federal Court under section 38 will effectively have to be re-litigated before the trial judge. This re-litigation is required because section 38.14 of the *Canada Evidence Act* requires the trial judge to accept the Federal Court order, but also requires the trial judge to determine if any additional order is appropriate to protect the accused's right to a fair trial in light of the non-disclosure order. Section 38.14 protects an accused's right to a fair trial. However, it places trial judges in the difficult position of deciding, on incomplete information, whether the right to a fair trial has been compromised by a Federal Court non-disclosure order.

There are serious and irremediable disadvantages to the current two-court system for resolving issues of national security confidentiality. The Federal Court is in the difficult position of having to assess what the defence needs for full answer and defence in the absence of any intimate familiarity with the issues in the criminal trial. The trial judge, on the other hand, is given the impossible task of assessing the importance of the undisclosed information to the defence –without any direct access to that information.

The Federal Court does not have full information about the trial, while the trial judge does not have full information about the secret information that is subject to a non-disclosure order. Section 38 litigation, as it currently occurs, delays and disrupts terrorism prosecutions, while leaving the trial judge to decide what, if any, remedy is necessary to compensate the accused for the lack of disclosure. The trial judge may have to rely on blunt remedies, including a stay of proceedings that will permanently end the prosecution. The trial judge is not able to revise the non-disclosure order, even though this power is considered to be critical in other countries that deal with the same issues of reconciling competing interests in disclosure and secrecy.

These problems are compounded by the delays to the criminal trial occasioned by the separate section 38 proceedings, and the possibility of appeals of section 38 issues to the Federal Court of Appeal and the Supreme Court of Canada. These interlocutory appeals can bring the criminal trial to a halt until they are resolved and may result in a mistrial because of unreasonable delay. Instead, there should be one decision-maker with access to all the relevant information and with the jurisdiction to make all the necessary findings and decisions. The current process in Canada, unique among Western democracies, needs to be changed.

Section 38 of the *Canada Evidence Act* should be amended so that claims of national security privilege in a trial of terrorism offences would be adjudicated by the trial judge as part of the criminal proceedings. Superior courts have constitutional jurisdiction to try criminal cases. Given the desirability of a single court, the most practical solution is to give the trial court jurisdiction over all aspects of disclosure and all claims of privilege. Appeals of decisions on section 38 claims should be allowed only after the verdict in the criminal trial.

The current procedure for dealing with section 38 claims does not allow the accused to participate, even though the decision about the claim may limit the disclosure of material that might help the accused's defence. The *Canada Evidence Act* should be amended to allow security-cleared "special advocates" to represent the interests of the accused, see the material for which the Attorney General of Canada is claiming national security privilege and, if warranted, challenge the claim. This role would be similar to that played by special advocates in immigration security certificate cases. Though passing information to clients would be prohibited, such special advocates would provide a much needed adversarial challenge to claims of national security privilege.

Special advocates would help to satisfy the constitutional right of an accused person to make full answer and defence. The accused would not be permitted to attend the hearing at which the privilege claim is determined or be informed about the information at contest unless the judge authorizes disclosure.

4.7 "Disclose or Dismiss": The Role of the Attorney General of Canada

At present, the Federal Court may, under section 38 of the *Canada Evidence Act*, order information to be disclosed despite a national security privilege claim by the Attorney General of Canada (AGC). However, the AGC can issue a certificate preventing disclosure that has been ordered. Besides the authority to override court orders, the AGC has powers relating to terrorism prosecutions. No terrorism charge can proceed without the Attorney General of Canada's consent.

The consequences of making these decisions are serious. The public interest should be the guiding factor in each case. Because the Attorney General of Canada already has the first and last word regarding terrorism criminal charges,

it stands to reason that the AGC should also be the ultimate decision-maker whenever the dilemma to disclose or dismiss arises.

Each of these powers of the Attorney General of Canada has stirred some controversy among critics who worry that the AGC's intervention can inject "politics" into what should be an "independent" judicial system. These criticisms do not stand up to scrutiny, because decisions made by the AGC are not based on partisan considerations. They can only be considered "political" in the broader sense that citizens in a democracy entrust their elected officials with the power to make decisions about the public interest in matters of national security.

Elected officials ultimately are responsible, with the Cabinet and the Prime Minister at the apex of that structure, to provide for the security of the nation. In addition to domestic consequences, national security decisions can have international ramifications, and therefore should not be made solely by the judiciary. The Attorney General of Canada, as Chief Law Officer of the Crown, is the appropriate official to bring both political authority and legal probity to decisions regarding terrorism criminal prosecutions that have an impact on the public interest.

In our legal and constitutional framework the ultimate decision-maker is the Attorney General of Canada. Where the decision truly is "disclose or dismiss," the current framework gets it right.

4.8 Source and Witness Protection

Law enforcement and intelligence agencies acknowledge that persons who provide information to them often do so at great risk to themselves and possibly to others close to them. Maintaining access to information from human sources may require the government to provide protection. Where individuals assisting the police are protected by police informer privilege, their identities are kept secret. If they do testify as witnesses, or if their identity is revealed inadvertently to their adversaries, these individuals can be protected through formal witness protection programs. In contrast, individuals who serve as sources to CSIS but who do not become witnesses do not have access to witness protection.

The Air India narrative demonstrates that, particularly when dealing with members of communities that may be preyed upon by extremists, individuals may often be willing to provide information to the authorities only if they are not required to expose their identities – by, for instance, testifying in a terrorism prosecution. The reluctance of sources to become witnesses is an important example of the problems caused by the traditional relationship between intelligence and evidence.

In terrorism cases, the current federal Witness Protection Program does not sufficiently address the multiple needs of witnesses and their families. The Commission recommends the creation of a position of "National Security

Witness Protection Coordinator" to deal with witness protection issues in terrorism matters.

One important responsibility of the Coordinator would be to determine who is allowed to enter the Witness Protection Program. The Coordinator could decide whether to offer protection to human sources and witnesses, and to their families, in criminal and intelligence investigations.

At present, the RCMP controls admission to the Program. Having the Coordinator make admission decisions would insulate decisions about protection of witnesses from decisions about investigations and prosecutions. It is not appropriate that a police agency with an interest in ensuring that sources agree to become witnesses make decisions about admission into a witness protection program. This is conflict of interest.

It is not clear whether police informer privilege extends to CSIS sources or, if it does not, whether it should. CSIS counterterrorism investigations are preventive. They often occur during the early stages of suspicious activities. CSIS may have difficulty determining whether its investigations will later uncover criminal behaviour that would warrant police investigation and criminal prosecution. Allowing CSIS to promise anonymity and to bring the privilege into play at that point might jeopardize subsequent terrorism prosecutions because those sources would not be able to testify. CSIS would perhaps be tempted to offer anonymity to assist it to collect intelligence, and much less interested in helping to make sources available to testify in terrorism prosecutions. This might lead to the privilege coming into play in particular situations in a way that serves the interests of CSIS, but not the broader public interest.

CSIS sources should nonetheless receive some protection against disclosure of their identities. The common law recognizes a category of privilege – the "Wigmore privilege" – that protects the confidentiality of information that is given in the expectation that it will be kept confidential, in circumstances when it is in the public interest to foster the type of relationship in which the confidential information was disclosed. At trial, the Wigmore privilege is typically invoked by the prosecution. However, the source may seek its protection if the prosecution does not.

Police informer privilege cannot be waived, except with the agreement of both the police and the informer. The informer alone can waive the Wigmore privilege, even if the party promising confidentiality (for instance, CSIS) does not agree.

4.9 Conclusion

Intelligence and law enforcement agencies both have legitimate, but sometimes competing, claims about how to use intelligence. Intelligence agencies may want to maintain the secrecy of the intelligence for operational reasons, while police agencies may want to see it made public as evidence in criminal prosecutions.

Neither claim trumps the other. The result is a tension between the two uses of intelligence. This is the "intelligence into evidence" conundrum.

Both types of agencies must re-examine their practices and procedures and find ways to avoid this dilemma. However, in some cases, a conflict will remain. The key is to ensure that, where a conflict remains about the possible disclosure of intelligence for a criminal prosecution, a single, independent decision-maker can resolve the conflict in the public interest. This decision-maker should have the experience, perspective and authority to transcend the narrower interests of the agencies involved. The recommendations in Volume Three are directed to changes in legislation, policy and procedure to assist in identifying and acting on this broader public interest.

VOLUME ONE
THE OVERVIEW

CHAPTER V: AVIATION SECURITY

5.0 Introduction

More than 24 years after the bombing of Air India Flight 182 and 8 years after the 9/11 attacks, terrorism against civil aviation remains a pressing global concern. Experts attribute this to the horrific and attention-getting results achieved through air terrorism: the sheer number of victims who can die as a result of a single attack and the fact that flag carriers can be seen as surrogates for countries. An attack on an airline whose planes display our flag, for example, may be seen as an attack on Canada itself. For these reasons, successful attacks on civil aviation yield high propaganda value, and vigilance in civil aviation security must continue so long as the terrorist threat remains.

The circumstances which permitted an unaccompanied, interlined bag to be placed on board Air India Flight 182, and to eventually destroy it, provide the context for the Commission's review of passenger and baggage screening and civil aviation security in general. One of the key lessons that emerges from the bombing is that security measures must be applied in mutually reinforcing layers in order to address all susceptibilities in the system. There is no one-size-fits-all solution. We must resign ourselves to the fact that terrorists will continuously probe the system's vulnerabilities. Similarly, we must close the remaining gaps in civil aviation security – some of which have been known for decades – before another tragedy occurs.

The evidence at the Commission's hearings bore out the experts' assertions that security must begin on the ground. There are limited options once an aircraft is airborne. This is demonstrated by the events leading up to the bombing of Air India Flight 182.

5.1 The Bombing of Air India Flight 182: A Multifaceted Failure of Aviation Security

The bomb that destroyed Air India Flight 182 on June 23, 1985, killing all 329 passengers and crew, was placed on the aircraft in Toronto in an unaccompanied, interlined bag. The bag containing the bomb began its journey in Vancouver on a Canadian Pacific Airlines (CP Air) flight to Toronto and was transferred ("interlined") to the Air India Boeing 747, in Toronto. Throughout its entire transport, the suitcase containing the bomb was not accompanied by any corresponding passenger. Less than an hour before the Air India bombing,

another unaccompanied suitcase containing a bomb exploded at Narita Airport in Japan, killing two baggage handlers and injuring four others. That suitcase had travelled from Vancouver to Narita on another CP Air flight and had also been interlined, destined for loading on an Air India flight to Bangkok. Although Air India was operating under an elevated threat level, CP Air was not informed of this fact and was operating under normal security protocols.

With today's knowledge of the threat of sabotage, a number of the circumstances that allowed for unaccompanied bags to be placed on both CP Air flights for interlining to Air India are alarming. In retrospect, the behaviour of those who booked and paid for the tickets and checked in the bags should have raised red flags, but a customer service mentality governed at the time, and airline staff were not instructed to watch for indicia of harmful intentions. The names on the reserved airline tickets were changed just prior to their purchase; a return ticket was switched to a one-way booking; the tickets were purchased within a few days of the flights; international tickets were paid for entirely in cash; demands to interline the bag destined for Air India Flight 182 were made in the absence of a reservation on that flight; and when the request to interline that bag met with resistance, the "passenger" identified as "M. Singh" became belligerent with the CP Air check-in counter staff at the Vancouver International Airport. Were it to occur now, some of this behaviour would be identified as presenting a possible threat as a result of airline ticketing surveillance measures that take place prior to the passenger's arrival at the airport. In fact, relenting to the demands of "M. Singh" to interline the bag without a reservation was contrary to industry practice and to CP Air's own security protocols, even as they existed in 1985.

The bombing of Air India Flight 182 was preventable but was made possible because of an unintentionally coordinated series of aviation security failures on the part of a number of stakeholders:

- CP Air failed to follow its own baggage security procedures;
- Both Air India and Transport Canada failed to appreciate the threat posed by unaccompanied, interlined bags;
- Air India was inexcusably careless in deploying checked baggage screening devices and procedures which it ought to have known were inadequate for the purpose, and failed to prevent unauthorized bags from being placed on its flights;
- Transport Canada, on behalf of the Government of Canada, failed in its role as regulator by neglecting to adapt the existing aviation security regime to confront the known terrorist threat of sabotage;
- Transport Canada also failed in its regulatory role by denying Air India the security support it required and by permitting Air India to rely on security procedures and plans that were inadequate to respond to the known threat of sabotage;

- Due to a climate of excessive secrecy nurtured by uncritical adherence to the "need-to-know" principle, crucially important intelligence was not shared, nor was it collected and analyzed in a coordinated manner; and
- Each of Air India, Transport Canada and the Royal Canadian Mounted Police (RCMP) failed to appropriately assess threat and intelligence information and to adequately communicate such information to relevant stakeholders.

The civil aviation security failures that permitted the bomb to be placed in the hold of the Air India Boeing 747 include a failure of screening technology and an over-reliance on it. The evidence at the inquiry demonstrated that Air India placed undue reliance on such technology, which consisted of Linescan X-ray devices and the Graseby PD4-C (PD4) hand-held explosives vapour and trace detector. At the time of the bombing, Air India's security plan for its Canadian operations included X-raying checked baggage as a standard security measure – an extraordinary requirement at the time. But by today's standards, X-ray technology of that era was both primitive and ineffective in screening for explosive devices. Metal items would appear as opaque, dark objects but, because of the quality of the images' resolution, careful attention and some interpretation were required on the part of the X-ray operators. These factors – which were known to authorities at the time – led the Commission's primary expert on civil aviation security, Rodney Wallis, to describe the use of X-ray equipment to screen for explosive devices in 1985 as a "…largely a cosmetic approach to baggage security" that "…lulled the public and some airline managements into a false sense of security." The PD4 was a flawed device that was unfit for use in detecting explosives, its singular purpose. In theory, the PD4 detected nitrated organic molecules, which would include nitro-glycerine and trinitrotoluene (commonly known as TNT). Testing at Lester B. Pearson International Airport on January 18, 1985 in the presence of officials from Transport Canada, the RCMP, the Peel Regional Police and Air India showed that it was ineffective in detecting gunpowder unless its probe was placed within one inch of the gunpowder sample.

The Air India flight that landed at and departed from Toronto on June 22, 1985 was known as Air India Flight 181, but after stopping at Mirabel International Airport, it became Air India Flight 182. In Toronto, all checked-in bags, as well as all interline bags from connecting flights were sent to the international baggage area for X-ray examination. After approximately two hours and fifteen minutes of operation, the X-ray machine broke down. The Air India security officer then directed the Burns International Security guards to use the PD4 to screen the remainder of the checked baggage for explosives. Apart from a cursory demonstration, the Burns guards had not been trained on the use of the PD4 and were unfamiliar with its operation. The evidence suggests that the PD4 sounded when brought close to some bags, but that this fact was not reported to the Burns supervisor and those bags were loaded onto the aircraft anyway. Whether the bag checked by "M. Singh" and interlined to Air India Flight 182 was

examined by X-ray before the machine malfunctioned or if it was examined by the PD4 afterwards cannot be determined.

In 1985, Canada was poorly prepared to defend against aviation terrorism, despite knowledge of the threat of sabotage and protective security measures. This country's aviation security regime was inadequate due to complacency, poor training and poor supervision of the private security guards hired to screen passengers and baggage. There was no such thing as a "security culture." The few security controls that applied to baggage were insufficient to meet the known threat of sabotage. In fact, security measures that could have prevented the suitcase containing the bomb from being placed on the flight were available, but were simply not implemented. The security regime of the day suffered from poor regulatory oversight, a lack of vigilance, a culture of complacency, an over-concern for customer convenience and a reactive approach to security threats. Despite a growing awareness that sabotage would be the terrorist's preferred means, aviation security measures were still focused on preventing hijacking. Except in certain cases of heightened threat, little emphasis was placed on the screening of checked baggage to be loaded in the hold of passenger aircraft.

5.2 From Hijacking to Sabotage: Evolution of the Terrorist Threat

Hijackings were the predominant threat to civil aviation in the 1960s and 1970s. The specialized United Nations agency with law-making authority in international civil aviation, was, and continues to be, the International Civil Aviation Organization (ICAO). It responded to the threat by adopting Annex 17 to the *Convention on International Civil Aviation* ("*Chicago Convention*"), the security annex entitled *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. The Annex sets out standards (adherence to which is required of states that are signatories to the Convention, known as "Contracting States") and recommended practices (which are in the nature of "best practices" or "desirable measures"). The standards were – and are – understood to be "minimum standards" that prosperous nations should exceed. Canada's domestic response included security measures that were designed to minimize the risk of hijackings. A 1973 amendment to the *Aeronautics Act* permitted regulations to be made for searching passengers, baggage and cargo. (The Act was amended again in 1976 to extend requirements to foreign aircraft.) The "no search, no fly" rule – fundamental to passenger and baggage screening – was included in the Act. This rule prohibited the boarding of commercial airliners unless authorized searches of persons and their belongings had been conducted.

The anti-hijacking measures appeared to have been effective. As of 1980, there had not been a successful hijacking in Canada since 1971, and none had been attempted since 1974. Hijackings around the world were declining by the late 1970s/early 1980s. By 1979, RCMP Security Service intelligence revealed that sabotage and bomb threats were of greater concern than hijackings. A 1980 Transport Canada report concluded that acts of sabotage posed the greatest threat to civil aviation in Canada. In that year, the Joint Study Committee on

Civil Aviation Security (whose membership included senior representatives of Transport Canada, the Air Transport Association of Canada and the RCMP) concluded:

> "…acts of sabotage rather than hijacking were perceived as the main threat…. As passenger screening procedures have proven to be an effective deterrent to prevent the carriage of unauthorized weapons and explosives in the aircraft cabin there is concern that persons are now attempting to place explosives in checked baggage, express parcel shipments, cargo and mail."

In recognition of the changing nature of the threat, Annex 17 was updated in 1981. Recommendation 4.1.14 provided that "…Contracting States should establish the necessary procedures required to prevent the unauthorized introduction of explosives or incendiary devices in baggage, cargo, mail and stores to be carried on board aircraft."

In 1982, Transport Canada conducted a study on air cargo and baggage security measures. A draft report was circulated in 1983. It recommended additional measures in high-level threat situations. The report also stated that all checked baggage should be manually searched or X-rayed and that all interlined baggage should be searched or scanned by X-ray. Unaccompanied baggage should be refused unless searched, sealed and held for 24 hours minimum. The Commission notes that some form of passenger-baggage reconciliation would have been required in order to identify unaccompanied baggage. Significantly, the report noted the temptation to relax security measures in light of tight funding and lack of terrorism incidents.

5.3 Domestic and International Responses to the Bombing

The Government of Canada responded quickly to the bombing of Air India Flight 182 by imposing passenger-baggage reconciliation and investing in new technology designed to assist in screening passengers and their baggage. In the weeks and months that followed the bombing, Transport Canada and the Government of Canada took further action to improve national aviation security. A rigid new Ministerial Directive was issued for all flights to Europe or Asia, requiring that all checked baggage be physically inspected or X-rayed, all cargo be held for 24 hours unless it was a perishable item from a known shipper, and all passengers and carry-on baggage be fully screened. The amended *Aeronautics Act* came into force on June 28, 1985, with updated aviation security regulations in December 1985.

Similarly, the international civil aviation community quickly responded to the bombing of Air India Flight 182 and the bombing at Narita Airport. The trade association for the world's international scheduled airlines, the International Air Transport Association (IATA) convened an extraordinary meeting of its

Security Advisory Committee (SAC) within days of the bombings. Led by Rodney Wallis, IATA's Director of Security at the time, the meeting resulted in a number of recommendations that brought about what Wallis described as "massive changes" in civil aviation security requirements around the world. The most significant of these was passenger-baggage reconciliation, the process by which passengers are matched with their baggage in order to prevent unauthorized baggage from being placed on board aircraft. A passenger and his or her baggage would be treated as a single entity. However, because IATA is an industry association, its recommendations reflect best practices and lack the force of law.

Properly implemented passenger-baggage reconciliation might well have prevented the bombing of Air India Flight 182. Had passenger-baggage reconciliation been conducted in relation to either the CP Air flight or Air India Flight 182, the bag containing the bomb should have been offloaded. In fact, a year earlier, in 1984, this process had been successfully employed in Canada by KLM Royal Dutch Airlines and CP Air in the context of a bomb threat, and had caused only minor delays.

ICAO also acted in the immediate aftermath of the bombings. As a result of a special meeting of ICAO's Ad Hoc Committee of Experts, Annex 17 to the *Chicago Convention* was amended to require that a form of passenger-baggage reconciliation be conducted by international air operators. However, what was eventually published as a standard in Annex 17 was flawed in that while it prohibited transportation of all baggage (including interlined baggage) belonging to passengers who registered but did not present themselves for boarding on international flights, it did not cover bags that were associated with passengers without a reservation. The unaccompanied bag that was transferred from the CP Air flight to the Air India flight in Toronto was not associated with a booked passenger. Given that the standard was adopted in response to the bombing of Air India Flight 182, it is ironic that compliance with this standard would not have prevented a recurrence of the same mistake that caused that disaster.

Canada was the first ICAO member country to require passenger-baggage reconciliation on international flights, in advance of the standard's publication. This measure was later extended to domestic flights.

But it was not until the bombing of Pan American World Airways (Pan Am) Flight 103 on December 21, 1988 over Lockerbie, Scotland – a copycat of the Air India Flight 182 bombing – that the international civil aviation community committed more fully to addressing the threat posed by the unaccompanied, interlined bag.

5.4 The Commission's Aviation Security Mandate

The Commission's aviation security mandate was to conduct an inquiry for the purpose of making findings and recommendations "…with respect to … whether

further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, particularly those relating to the screening of passengers and their baggage." However, early in the Commission's work, it became apparent that a narrow focus on passenger and baggage screening would not provide assurance that all of the deficiencies that led to the bombing had been addressed. In addition, longstanding gaps in civil aviation security were identified. Terrorists probe the system for weaknesses that they can use to their own advantage. Anything and anyone that has access to the aircraft must be secured to the extent that is possible, given predetermined levels of acceptable risk for all areas of vulnerability. A holistic approach to security is required, and the same approach was required of the Commission.

The next act of sabotage against civil aviation in Canada could well have air cargo as its target. Carried primarily on passenger aircraft, an attractive target for terrorists, air cargo in this country is neither routinely searched prior to loading, nor subjected to adequate screening measures. In many respects, air cargo security today is strikingly similar to the checked baggage security regime as it existed prior to the loss of Air India Flight 182. In contrast to the multi-layered approach to screening passengers and their baggage, air cargo is generally placed alongside baggage in the aircraft hold so long as the shipper meets the minimal criteria of having had a regular business relationship with the air carrier. This brings to mind the image of fully screened passengers seated on aircraft with largely unscreened air cargo perhaps one metre beneath them. Improvements to passenger and baggage screening measures that are aimed at preventing a concealed bomb from being placed aboard passenger aircraft are pointless if that bomb can still be directed on board the same plane hidden in cargo that has not been X-rayed. The inadequate approach to air cargo was the single most disturbing revelation about the remaining deficiencies in Canada's civil aviation security regime. In addition, evidence at the Commission's hearings disclosed serious weaknesses in airport security that could undermine the defence provided by passenger and baggage screening.

As a result, and with the approval of the government, the Commission interpreted the aviation security aspect of its mandate broadly, and considered a wide range of issues including air cargo security, non-passenger screening (NPS), and the particular challenges presented by Fixed Base Operations (FBOs) and General Aviation (GA).

5.5 Passenger and Baggage Screening Today

Passenger and baggage screening is now much more comprehensive than it was in 1985. Creation of the Canadian Air Transport Security Authority (CATSA) on April 1, 2002 represented a significant improvement in screening passengers and baggage. In November 2002, CATSA, a Crown corporation, became responsible for effective, efficient and consistent screening nationwide of all persons accessing aircraft or airport restricted areas through screening points, as well as their belongings and baggage. This is referred to as pre-board screening,

or PBS. As of January 1, 2006, 100 per cent of checked bags for flights departing Canadian airports were screened with explosives-detection equipment. CATSA now screens 37 million passengers and 60 million pieces of luggage at Canadian airports each year. Hold bag screening, or HBS, is accomplished through multiple layers of screening that involve both automated detection, using state-of-the-art detection equipment, and human skill and judgment. X-ray machines, computed tomography (CT or CAT) devices and explosives trace detection technology are all used for PBS and HBS. At the heart of both PBS and HBS is the "no search, no fly" principle.

Unlike the low-powered, low-resolution X-ray machines used in 1985, the devices now used to scan baggage employ two X-ray beams at different energy levels, allowing differentiation between organic and inorganic materials within an object being scanned. The images are displayed on high-resolution monitors and colour-enhanced in a manner that makes them stand out from surrounding materials. Alertness in screeners involved in PBS is maintained through a training and motivational tool that randomly projects the image of a weapon, or of an explosive device or substance.

CATSA contracts screening operations to independent service providers. The contracted service delivery model fulfills CATSA's objectives at a reasonable cost. However, contracted service providers – and by extension, CATSA – have encountered significant difficulties in recruiting and retaining screening personnel. This is an ongoing problem that has resulted in staffing shortfalls and complicates training programs.

In some foreign jurisdictions, screeners search passengers and baggage for large amounts of currency and illicit items such as narcotics, in addition to weapons and substances that are potentially dangerous to civil aviation. The sole focus of CATSA screeners, however, must remain that of civil aviation security. The task of identifying weapons and improvised explosive devices before they are placed on aircraft is simply too important to be shared with other functions.

Screening points must be tested to assist in identifying weaknesses in the system, whether these occur in the form of technical deficiencies or as a result of human failure. Effective follow-up is essential. This testing includes infiltration tests conducted by Transport Canada security inspectors, who attempt to bring concealed weapons or explosive devices through PBS check points. Infiltration test failures result in CATSA receiving an "enforcement letter," advising of the failure and requiring a written response explaining how that failure is being addressed. CATSA's responses to an enforcement letter can include decertification of the screening officer(s) involved, which necessitates retraining or "de-designation" of such officer(s). The Standing Senate Committee on National Security and Defence (Senate Committee) has recommended that a summary of intrusion test results be released to the public after some reasonable period during which the deficiencies could be addressed. Ultimately, the evidence at the

inquiry did not clearly demonstrate the need to disclose infiltration test results but, nonetheless, there must be continual pressure on all parties to ensure that deficiencies are quickly addressed – in order to justify the public's investment in CATSA and its confidence in our aviation security regime.

Currently, there is a trend in passenger screening that marks a move toward identifying individuals with hostile intent. This trend is exemplified by ongoing interest in behavioural analysis, which is already being practised to a limited extent, and by creation of the Passenger Protect Program (PPP).

Behavioural analysis is a form of PBS that involves monitoring passengers for atypical or suspicious behavioural patterns or attributes that suggest that those passengers may present a risk to civil aviation and should therefore be subjected to more rigorous questioning. Proponents of behavioural analysis contend that it screens individuals for potentially hostile intent, and that, where practised, it provides another necessary layer in the multi-layered approach that is essential to civil aviation security. In fact, it is reasonable to conclude that, had some method of behavioural analysis been used in 1985, the behaviour of "M. Singh" may have triggered greater vigilance and prevented the bombing of Air India Flight 182. Today, the airline industry monitors ticket purchasing patterns using tools that were not available in 1985. Relevant factors include payment in cash through third parties, one-way bookings and certain travel destinations. However, analysis of behaviour observed at the airport terminal raises a number of concerns, most notably the difficulty in constructing an effective and accurate tool that respects individual rights and is not prone to abuse. There is a fine line between behavioural criteria and those which amount to racial profiling.

Behavioural analysis has been used in civil aviation security by other countries, notably Israel. To some extent, it is already practised in Canada in that it is used to observe passengers by Aircraft Protective Officers (APOs), the armed RCMP officers who provide covert security on select flights. However, if behavioural analysis were to be used in PBS, a high degree of discretion would have to be assigned to CATSA's frontline personnel. In the end, the Commission shared the conclusion of the *CATSA Act* Review Advisory Panel (CATSA Advisory Panel) that, prior to any adoption of this measure as part of PBS, international experiences with this method must be thoroughly reviewed. In addition, the accuracy of the process and the competencies and training required must be carefully assessed.

The PPP created and maintains Canada's no-fly list. Under this program, which was launched on June 18, 2007, the Minister of Transport, Infrastructure and Communities can deny boarding privileges to any passenger the Minister believes poses an "immediate threat to aviation security." The PPP has been criticized by the Privacy Commissioner of Canada and her provincial and territorial counterparts, who have questioned the rationale for the program, as well as the lack of transparency in the process by which individuals are selected for inclusion on the no-fly list, which is known as the Specified Persons List (SPL). The SPL is created by an advisory group that includes the RCMP and

the Canadian Security Intelligence Service (CSIS), and is updated regularly. Criteria for inclusion in the SPL are not set out in legislation but are simply provided as public information on Transport Canada's website. The Office of the Privacy Commissioner has questioned the rigour with which foreign-sourced information provided by the RCMP and CSIS to other advisory group members will be evaluated. An individual who is denied boarding privileges receives an emergency direction that is in force for 72 hours. He or she is also referred to the Office of Reconsideration, which is part of Transport Canada. The reconsideration process has been heavily criticized for its lack of a legislative basis, for failure to provide the information underlying the decision, for failure to provide an oral hearing and for the fact that the final decision is made by the Minister – the same official who made the initial determination to deny boarding privileges.

To date, there has been only one denial of boarding privileges under this program: in June 2008. The person who was denied boarding has instituted an application for judicial review, which includes a contention that the PPP violates his *Charter* rights to freedom of movement and due process.

In time, the value of this program – which may include offering a degree of reassurance to other countries that Canada has a robust aviation security regime – may be shown to be significant. However, that has yet to be demonstrated.

5.6 The Long-Standing Inadequacy of Canada's Air Cargo Security Measures

Much criticism was directed at the Government of Canada by witnesses at the Commission for the long delay in addressing the known gap in air cargo security. Air cargo was recognized in Canada as being vulnerable to sabotage by terrorists, both prior to 1985 and in the immediate aftermath of the bombing of Air India Flight 182.

The international civil aviation community also recognized the risk posed by cargo in the wake of the Air India and Pan Am losses, and acted quickly to devise a viable solution for securing cargo for air transport. Following the bombing of Pan Am Flight 103 over Lockerbie, Scotland, an amendment to Annex 17 encouraged ICAO Contracting States to implement a system of regulated agents in order to ensure the security of cargo by those entities handling cargo prior to its arrival at the airport. The United Kingdom and many other European countries followed suit, developing regulated agent systems that were highly lauded by the aviation security experts who appeared at the present Commission's hearings. Many of these same countries are also utilizing advanced screening technologies for searching air cargo.

To date, however, Canada has failed to incorporate such systems, including X-raying cargo, into its aviation security regime, despite knowledge of the deficiencies in the existing air cargo security program and despite ICAO's recommendations. Although there is a system of known shippers in Canada,

this term is outdated and, more importantly, has been misinterpreted and used to refer to entities that have only a cursory business relationship with air carriers. Contrary to the Annex 17 definition of regulated agents, there is no requirement in Canada for known shippers to apply security controls to cargo in their care, nor is there a requirement for government oversight. Cargo is not systematically searched by air carriers, which constitute the only stakeholder charged with the responsibility for searching cargo, and there is little access to any technological equipment for this purpose. There was no evidence to suggest that any training is provided for cargo searching in Canada and concerns have also been raised about airside access to, and monitoring of, cargo.

Air cargo has been left dangerously exposed to the threat of bombs, explosive devices and other methods of unlawful interference. It has been 29 years since bombs were first recognized as the major threat to civil aviation, and still this threat has yet to be comprehensively addressed. While passengers and baggage continue to provide means by which bombs may be placed aboard aircraft, both are subjected to thorough screening processes. Air cargo is not. Viewed in this manner, cargo is less the "next threat" than it is the "last war" that is still being fought, albeit ineptly. To be truly effective the "war" must be fought on all major fronts, not just a chosen few.

By 1991, at the time Annex 17 was amended to include the definition of the known shipper (which was later changed to "regulated agent"), Canada had intimate knowledge of the seriousness of the risk posed by air cargo and should have taken steps to address this gap in aviation security. In 2009, some 18 years later, virtually no changes have been implemented to enhance the security of air cargo.

While harmonization with international partners is a desirable objective, and responding positively to recommendations from ICAO is expected, air cargo security should not be driven by the intervention or inducement of others. Air cargo has been recognized as a weakness in aviation security in Canada since the 1980s, yet Canada chose not to begin addressing this gap until 2004, at a time when cargo security had become a greater priority in the United States. It is difficult to shake the appearance that progress in air cargo security in Canada has been prompted by external influences from the international civil aviation community, through ICAO, and because of developments in Canada's largest trading partner, the United States. Yet the United States itself has come under fire for not moving more quickly on securing air cargo since the issue was identified in 1996 by the Gore Commission. Deficiencies in security cannot await the slow movement of others.

Such deficiencies, which had grave consequences in 1985, have direct application to the current context of air cargo security. Cargo represents a significant risk to civil aviation and great care must be taken not to repeat previous mistakes. The Commission's mandate requires consideration of whether a civil aviation security regime is in place that will assure the security of those who come into

contact with civil aviation and whether an effective regime exists to thwart possible terrorist attempts to breach the security barriers as erected. With the knowledge that cargo is susceptible, vulnerable and inadequately protected, it is imperative that connections to the past are drawn.

The statistics alone demonstrate the need for a more effective approach to air cargo security. In Canada, almost 80 per cent of air cargo is transported on passenger aircraft. There are 30 million potential shippers, approximately 2 million shippers for all-cargo aircraft, 20,000-30,000 frequent shippers and 750-1500 freight forwarders (approximately 250 of whom belong to Canadian International Freight Forwarder Association (CIFFA)).

Federal Budget 2009 pledged funding to a new air cargo security initiative. The Commission supports a comprehensive initiative that not only complies with Canada's international treaty obligations, but meets or exceeds international best practices. The Commission urges that this initiative be implemented expeditiously.

5.7 Improving Airport Security

Measures aimed at protecting the airport environment are fundamental to a properly functioning civil aviation security regime. The bombing of Air India Flight 182 revealed important weaknesses in airport security, including problems with access control, airport security plans, perimeter security and general security awareness.

Airports represent the hub of civil aviation, where industry, the government and the public interface. Virtually all aviation security measures, including passenger and baggage screening, are conducted at the airport, which essentially functions as a physical barrier to the aircraft. In a multi-layered approach to aviation security, the airport must provide a protective environment that supports, complements and preserves the integrity of all other security measures. To do otherwise leaves the aircraft, with its passengers and crew, vulnerable to attack.

Quite apart from the sabotage of aircraft, air terminals themselves are targets of aviation terrorism. Long line-ups and passenger congestion at airline check-in and security counters cause large numbers of people to assemble in a confined area, creating target-rich environments that are ripe for attack. There have been a number of significant attacks on airports throughout the history of aviation terrorism. As security defences to safeguard the aircraft are strengthened through the application of comprehensive measures and the use of increasingly sophisticated technology, terrorists will be deterred from attempting to place bombs on aircraft because of the unlikelihood of success. Instead, they will turn to other civil aviation targets to achieve their objectives, probing for areas of weakness that can be exploited to their advantage. Canadian airports provide these in abundance, and the airport terminal is one such area.

The Commission learned that significant deficiencies have long characterized airport security in Canada. In particular, access to airside and restricted areas of airports are poorly controlled. In contrast to the comprehensive, multi-tiered screening process in the airport terminal, to which all passengers and baggage are subjected prior to being permitted aboard aircraft, the system for screening non-passengers who access restricted areas of airports, along with their belongings, lacks rigour and can be easily circumvented. Lax perimeter security also allows vehicles and their occupants to enter airside portions of the airport with minimal, if any, screening. There is evidence to suggest that, once on airport property, the movement of such vehicles is not carefully monitored. As a result, despite impressive efforts to safeguard the aircraft against sabotage from passengers and baggage, opportunities remain for bombs to be placed aboard aircraft by other means.

Weaknesses in airport security, together with shortcomings in air cargo, Fixed Base Operation (FBO) and General Aviation (GA) security, have created a real anomaly in Canada's defence against air terrorism. Charter and air cargo services at FBOs and GA facilities, often involve wide-body aircraft, but unlike similar aircraft arriving at and departing from the air terminals, their crews, passengers and cargo are unscreened. As such, FBOs and the GA sector present ready targets for terrorists. The result is that fortress-like security is applied to the front, more publicly visible side of civil aviation, while the side that is more hidden from public scrutiny remains exposed. The Senate Committee likens the current status of aviation security in Canada to a house in which "…the front door…[is] fairly well secured, with the side and back doors wide open."

That this situation persists is made all the more remarkable by the fact that, following the loss of Air India Flight 182, airport security was also considered a priority in Canada. On July 4, 1985, eleven days after the bombing, Transport Canada's Deputy Minister requested an audit of airport security at Vancouver, Pearson and Mirabel International Airports – the very airports in Canada through which the bomb had journeyed. The audit report was completed on July 24, 1985, and revealed a number of serious deficiencies at all three airports. Common themes included inadequate protection of the aircraft, inadequate control of access to restricted areas, deficiencies in airport security plans and the need for improved security awareness – all themes that experts have continued to highlight as problems today.

Over twenty years have passed, but many of the same deficiencies, including inadequate access control, that were noted in 1985 by the airport security audit report and the Seaborn Report – a seminal document in Canadian aviation security and blueprint for further action in this field – continue to be raised as urgent concerns today. Many solutions similar to those proposed so long ago are now being proposed as basic requirements for bringing airport security to an appropriate level. Even though the Seaborn Report was presented as a strategic action plan for the Government of Canada in relation to aviation security, action has been slow in coming. However, Budget 2009 included $2.9 million in funding for the development of aviation security plans, with

priority being given to the "initiation of airport security plans" as a result of pilot projects conducted at several airports in the past year. Budget 2009 also provided funding to hire additional oversight officers. Virtually all stakeholders and experts recommended the development of security awareness programs at airports, and various solutions have been proposed for improving access control.

It is true that some strides have been made in relation to airport security, particularly since the terrorist attacks of September 11, 2001. These improvements have included the creation of CATSA, which in November 2002 was given the responsibility for the random screening of non-passengers and for developing the biometric Restricted Area Identification Card (RAIC). The RAIC system has still not been fully implemented at airports across Canada, but is regarded internationally as a very sound security measure. In addition, airport security has been improved in the post-9/11 era in the form of covert security provided by APOs, who are armed and well-trained RCMP officers deployed through the Canadian Air Carrier Protective Program (CACPP). Although their primary function is to protect high risk flights while airborne, APOs provide an additional element of security in the airport environment. Recognizing the growing security concerns surrounding the airport environment, the CACPP training program is evolving to provide greater emphasis on such issues. The CACPP has drawn praise from the international civil aviation security community. The fact remains, however, that much more needs to be done to buttress airport security in Canada.

5.8 Identifying the Threat: Past, Present and Future

To be effective, security must be both retrospective and pro-active. That may seem like a contradiction in terms. However, a consistent theme throughout the history of aviation terrorism is that vulnerabilities are known long in advance, but measures are not implemented to meet the threats until an incident occurs. As Rodney Wallis has written,

> Hindsight is a great blessing. History provides an opportunity for turning hindsight into foresight. Hands-on experience gained in a variety of countries helps in the development of security defenses. All security executives should have this experience and be avid students of what has gone on before. It will help them predict and prevent incidents occurring in the future. It will also go a long way to making the skies safer for passengers and crews and for people on the ground. Security managers must always be open to innovative ideas and be unafraid to experiment in the interest of passenger security.

The failure to adjust to the shift in threat from hijacking to sabotage and to the corresponding threat of bombs in baggage is just one example of a reactive approach that has plagued civil aviation security from the very beginning.

Another is the failure to adopt measures to counter the threat posed by liquid explosives. The measures so quickly implemented to address a threat posed by liquid and gel explosives in August 2006 actually addressed a threat that had been known to exist for almost two decades. Even the phenomenon of the suicidal hijacker existed before the events of September 11, 2001. Continuously and repeatedly, lessons fail to be learned.

5.9 Use of Intelligence

To be effective, an aviation security program must be intelligence-led, be based upon up-to-date threat assessments and be resilient enough to adapt to new threats as they emerge. It is apparent that steps have been taken toward correcting the intelligence failures that contributed to the bombing of Air India Flight 182. Those failures were due, in part, to excessive secrecy and the institutional preoccupation with the "need-to-know" principle. After the September 11, 2001, terrorist attacks, Canada's intelligence community moved away from uncritical adherence to that principle and accepted that, in many circumstances, the need to share must prevail. On an institutional level, this has resulted in creation of the Integrated Threat Assessment Centre (ITAC), an organization established in October 2004 and staffed by representatives of numerous government agencies. ITAC produces comprehensive threat assessments focused exclusively on terrorism. No such integrated intelligence capacity existed in 1985.

CATSA has maintained that it lacks sufficient access to the intelligence it considers essential to its operations and has sought to participate in ITAC. Although both CATSA and the Senate Committee have argued that CATSA should be permitted to develop its own intelligence capabilities, the Commission agreed with the CATSA Advisory Panel that Transport Canada remains the most appropriate channel for receiving strategic intelligence information regarding terrorism and disseminating relevant intelligence to CATSA as a consumer. As long as relevant intelligence is provided by Transport Canada, there is no need for CATSA to go beyond its core screening mandate in order to "re-invent the wheel" by developing an intelligence function. However, there is considerable value in providing front line personnel with usable, actionable intelligence through regular briefings or security updates. This is already occurring, and should be encouraged. This intelligence sharing keeps front line personnel up to date with current threats but also boosts their motivation and morale, as well as fostering a genuine sense of mission.

5.10 Risk Management

Risk has been defined as the "chance of loss or harm" or the "probability that some discrete type of adverse effect will occur." Threat, which is present in security-related risk, is an expression of intention to inflict evil, injury or damage.

A proactive approach to risk management is essential for a robust civil aviation security regime. The object of risk management is to reduce risk to a

predetermined and acceptable level (often described as "as low as reasonably achievable" or ALARA). This object is attained by applying a reliable method for identifying the highest priority risks in order to determine appropriate risk control measures. This in turn assists in allocating resources in a cost-effective manner.

In 1985, the risk of sabotage against Air India would have ranked highly in a risk matrix. Moreover, risk management processes used at the time should have identified the June 1st Telex as having a significant impact on the perceived risk. The telex, sent to all Air India stations on June 1, 1985, contained a threat advisory from Air India's Chief of Vigilance and Security Manager. It was based on intelligence obtained by the government of India and reported that Sikh extremists were likely to sabotage Air India aircraft by means of time-delayed explosives being placed in the cabin or in checked baggage. It directed all Air India stations to implement counter-sabotage measures for flights at all airports. However, this telex was not shared with Transport Canada, and decisions were made to employ methods that were known to be of questionable value for the risk faced, or to waive protective measures where there should have been no discretion.

The terms "risk-based approach" and "risk assessment" were used liberally throughout the Commission's hearings, but at times, those who used these phrases offered little explanation or had little apparent regard for their precise meaning. This may have created an illusion of rigour where the evidence may, in some instances, suggest otherwise. When pressed, Transport Canada officials were unable to articulate a consistent means by which that Department manages risk in civil aviation security. Public confidence in civil aviation security demands that institutions with responsibility in this area provide adequate disclosure of the methods they use to manage risk.

In addition, although civil aviation security is a shared responsibility amongst numerous stakeholders, there was little evidence of a coordinated, system-wide risk management strategy.

The Commission has concluded that, in the absence of a systematic approach to risk management, there is cause for concern that significant risks in civil aviation security may go unnoticed.

5.11 Oversight of Aviation Security

Annex 17 to the Chicago Convention requires each signatory state to designate a domestic agency responsible for its civil aviation security program. Despite the conclusion reached by the Senate Committee, the Commission agrees with the CATSA Advisory Panel that Transport Canada should remain the designated authority responsible for Canada's national civil aviation security program.

Proper oversight requires the development and maintenance, by Transport Canada, of a robust aviation security regime that adequately addresses all

significant threats. To do so, the regime must not only meet but exceed Annex 17 standards wherever possible, embracing its tenets in the spirit with which its provisions are intended, and must be informed by international best practices. The system must be continuously monitored to ensure that it remains capable of thwarting terrorist threats or that adjustments can be made, as necessary, on a timely basis. The system must include a carefully considered plan for responding to true emergencies.

A sufficiently robust regime can be achieved by ongoing adherence to a number of key principles that were frequently referenced by the experts and industry stakeholders who appeared before the Commission. Some of these principles have already been discussed. They include ensuring that lessons from the past are understood, along with trends and patterns in global air terrorism; implementing measures in a proactive manner, establishing a multi-layered system of security; providing for flexible, performance-based measures where suitable, fostering a culture of security awareness, and, importantly, determining the relative need for security measures through the systematic application of accepted risk management protocols, on both an individual and global basis. The regime must be constantly scrutinized as to its effectiveness in the context of past, present and future threats, including threats that arise in other parts of the world.

Annex 17 requires that each signatory state establish and implement a written national civil aviation security program. Transport Canada has no specific document describing Canada's civil aviation security program in its entirety. Instead, Transport Canada takes the position that it possesses the equivalent of a national program as envisioned by the standard in the form of a substantial body of documents. These documents include all legislative and regulatory instruments and other documents relating to civil aviation security requirements in this country. But precisely because civil aviation is a shared responsibility, a premium should be placed on the clarity and coordination that would be provided by a single articulation of the entire regime. Such a document should set out the full slate of civil aviation security policies and procedures and each entity's role in their implementation. A national civil aviation security program will enhance the ability of each entity (be it a government agency or department, or an industry stakeholder) to comply with the national program and to develop its own program, as required by Annex 17.

Consistent with its view that there exist deficiencies in aviation security, the Commission concluded that Canada's regulatory framework for civil aviation security does not meet all of the minimum standards outlined in Annex 17. Standard 4.1 requires Contracting States to establish measures to prevent unauthorized explosives and other dangerous devices or substances from being introduced on board civil aviation aircraft "by any means whatsoever." At present, Canadian civil aviation security is not sufficiently comprehensive to meet this standard. Civil aviation remains vulnerable to acts of unlawful interference because it is still possible to introduce bombs and other weapons of sabotage on board aircraft by cargo and means other than by passengers and baggage, contrary to Standard 4.1.

Transport Canada has launched an initiative to review the national civil aviation security regulatory regime in its entirety. This is a welcome and important development, and must be an urgent priority of the Government of Canada. Where a significant vulnerability is identified, Canada must strive for timely solutions and must not defer its response until measures are imposed by other regimes or, worse, by another act of air terrorism.

Oversight in civil aviation security must involve rigorous mechanisms of inspection and enforcement of established security procedures, which requires ongoing government commitment.

5.12 Limits on Civil Aviation Security

Security is not absolute. Resources are limited and other factors need to be considered as well, including the efficiency of air travel and the rights of individuals. In addition, some measures are required as a result of international obligations, both legal and practical. Security measures must, therefore, be chosen on the basis of risk management principles that are themselves based on nationally/internationally accepted standards. Limited resources must be distributed across all areas of risk to achieve an overall acceptable level of security. Both past and anticipated threats must be accounted for. Care should be taken to ensure that the necessary rigour and meaning are given to the mantra – often used by those responsible for civil aviation security – that a "risk-based approach" to civil aviation security is required.

5.13 Duty to Warn

No hindsight is necessary to conclude that threat communication among those responsible for aviation security was starkly deficient in 1985. The Government of Canada and Air India were both aware of the terrorist threat faced by Air India, but neither of them ensured that other civil aviation stakeholders were aware of that threat. If air carriers interlining passengers and baggage to Air India had been made aware of the threat faced by Air India, they might well have altered their security operations. Had CP Air been informed of that threat, it might have exercised greater vigilance about interlining the "M. Singh" bag in the absence of a reservation on Air India Flight 182. Today, Transport Canada would inform other air carriers of threats to a target airline or aircraft to which passengers may be interlined.

The Commission was invited to conclude that government officials have a legal or ethical duty to warn the public about threats against airlines. However, it is difficult to articulate the threshold that must be met before a warning should be given. Ultimately, the Commission concluded that important information about security threats and measures should be shared with the public in a manner that promotes overall security.

5.14 Funding Aviation Security

The issue of who should pay for aviation security has long been debated. For at least two decades, IATA has argued that this should be a responsibility of national governments, due to the fact that, since airlines have national flags on their tails, they amount to a small piece of the target country. There is force to this argument. Aviation security is a core function that is directly related to national security. As such, funding must be derived primarily from government.

Government funding can include funds obtained through the user-pay principle, as exemplified by the Air Travellers Security Charge (ATSC), first imposed in 2002. However, the ATSC has well-founded criticism. It lacks transparency, and funds generated by this charge are not directly applied to aviation security concerns. Regardless of the precise means by which aviation security is to be funded, new initiatives to address the gaps in Canada's aviation security regime will require both an initial influx of funding and an ongoing commitment on the government's part.

The reality is that aviation security incidents themselves are costly events, and prevention is the more economical option.

5.15 Conclusion

Despite the passage of 24 years since the bombing of Air India Flight 182, deficiencies continue to exist in Canada's civil aviation security regime. Improvements in screening passengers and their baggage have been necessary and important, but those improvements may have come at the cost of addressing gaps elsewhere in aviation security. Deficiencies in other areas must be addressed as soon as possible. It would be unfortunate if Air India Flight 182's legacy to Canada's civil aviation security regime were to be narrowly focused on passenger and baggage screening. Some of these gaps have existed for so long that further inaction is both dangerous and unconscionable. The Government of Canada has recently moved to address some of these gaps – notably in relation to air cargo security – but increased momentum is essential. Independent reporting by government watchdogs, such as the Standing Senate Committee on National Security and Defence and the Auditor General of Canada, will help to sustain that momentum but, because of the dynamic nature of civil aviation security and the record of successive governments in delaying action in this field, the Commission recommends that a formal, independent review of Canada's civil aviation security regime should take place every five years. More detailed recommendations can be found in Volume Four.

VOLUME ONE
THE OVERVIEW

CHAPTER VI: TERRORIST FINANCING

6.0 Introduction

Before 2001, Canada did not expressly prohibit terrorist financing. The 2001 *Anti-terrorism Act* (ATA)[1] introduced specific crimes relating to the financing of terrorism, and provisions to allow the revocation of the charitable status of any charity involved in terrorism. It also added combatting terrorist financing to the mandate of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

These laws and the implementation of other government initiatives are no guarantee of success. Until very recently, these laws yielded few successful terrorist financing prosecutions.

The struggle to curtail the financing of terrorism is an uphill battle. One impediment is the small cost of terrorist acts. It has been estimated that the bombing of Air India Flight 182, which claimed 329 lives, probably cost the perpetrators less than $10,000. The direct costs of the 2004 Madrid train bombings which claimed 191 lives have been estimated at €15,000.

The methods to acquire and move the small sums necessary for terrorism are limitless. They include direct fundraising, extortion, the use of charities and not-for-profit organizations, legitimate employment and business income, organized crime and state support. There are near infinite means to move those funds through formal and informal financial institutions, as well as physically through the use of trusted couriers.

Currently, much of Canada's anti-terrorist financing initiative is based on a money laundering model that focuses on transactions over $10,000. This model is not well-suited to terrorist financing.

Laws against terrorist financing are at best a limited tool. If one sector such as financial institutions is regulated, terrorists can quickly move to another sector such as informal money transfer systems. Revoking the charitable status of a charity may not impair the flow of funds since donors to extremist causes are unlikely to be deterred by the loss of a tax receipt. The former charity may survive nicely as a non-registered, not-for-profit entity that continues to channel funds to terrorists.

---

1 S.C. 2001, c. 41.

Currently, Canada is not making optimal use of the extensive and costly measures that it has taken against terrorist financing. Agencies responsible for combating terrorist financing, most notably the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and the Canada Revenue Agency (CRA), which deals with charities, are not sufficiently integrated into the intelligence cycle to detect terrorist financing or to provide the best financial intelligence to CSIS and the RCMP. Moreover, transactions involving the small sums needed to finance terrorist acts are not likely to be discovered through the routine collection and processing of information by FINTRAC and the CRA.

Discovering terrorist financing activity amidst millions of reports about financial transactions or thousands of applications for charitable status is like finding the proverbial needle in a haystack. It will often be necessary for FINTRAC and the CRA to be guided in this search by intelligence from CSIS, CSE and their foreign partners, as well as by tips from the RCMP. At the same time, FINTRAC and, to a lesser extent, the CRA face restrictions on the information they are free to share with other agencies. Both are "arms length" bodies because of their obligations to protect the confidentiality of the information they collect. There are some legitimate needs to protect the financial and taxpayer information they possess, as well as legislated restrictions on what they can pass on to other agencies. Nonetheless, there may be a need to redress the balance between privacy and openness to reconsider some restrictions in order to accommodate legitimate needs for information sharing.

6.1 The Importance of Legislating Against Terrorist Financing

Although laws against terrorist financing may not be the most effective instrument to prevent terrorism, they are a practical necessity. Canada ratified the *International Convention for the Suppression of the Financing of Terrorism* in 2001. Various UN Security Council resolutions commit Canada to taking efforts to prevent and suppress terrorist financing. Canada should and does take these international obligations seriously.

The G7 countries established the Financial Action Task Force (FATF) as an inter-governmental body. FATF standards have been endorsed by more than 170 jurisdictions. Canada must live up to these standards. The international community has recognized that, in a world with increasing globalization, all countries must take steps to ensure that they do not become safe havens for terrorist financing. If one country does not do its share, the success of the entire global fight against terrorist financing is jeopardized.

The freezing of assets or the launching of a terrorist financing prosecution may be useful means to disrupt a terrorist network long before any act of terrorism has been committed. Professor Bruce Hoffman warned that the failure by the authorities to actively counter terrorist fundraising activities also means "consigning [ethnic and religious] communities to be preyed upon by their co-religionist [brethren] or by their ethnic brethren."[2]

---

2 Testimony of Bruce Hoffman, vol. 19, March 9, 2007, p. 1842.

The intelligence produced by initiatives against terrorist financing is increasingly recognized as a valuable asset in global terrorism investigations. More raw intelligence on individuals (and thus terrorists) is available in the financial databases of the Western world than in any other database. Financial intelligence provides a means to identify the networks that support terrorism, as well as the links between people, organizations and even countries.

6.2 The 2001 and 2006 Reforms

The 2001 *Anti-terrorism Act* amended the *Criminal Code* to prohibit terrorist financing and to provide for court-ordered freezing of terrorist assets. Parliament gave an existing entity, FINTRAC, the mandate to collect and analyze financial data to enable it to assist in the detection, prevention and deterrence of terrorist financing. FINTRAC's governing legislation, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), imposes record keeping and reporting requirements, primarily on private sector entities. It also permits FINTRAC to receive information provided to it voluntarily by other agencies and to disclose certain information to agencies specified in the legislation. Canada's regime to combat terrorist financing depends on the sharing of information between various agencies as well as the reporting by the private sector of suspicious and other transactions.

The ATA also created the *Charities Registration (Security Information) Act* (CRSIA), which provides for the use of classified information to justify a decision to revoke the charitable status of an organization, without disclosing that information to the organization.

In late 2006, additional legislation was enacted to respond to deficiencies in Canada's terrorist financing laws. The new legislation creates a registration regime for money services businesses. It strengthens the client identification process required in the case of wire transfers, strengthens measures against the use of charitable organizations for terrorist financing, and enhances CRA's authority to disclose information to disclose information to CSIS, the RCMP and FINTRAC.

6.3 The Money Laundering Model

Although there are similarities between money laundering and terrorist financing, the differences outnumber the similarities. In money laundering, the money has been accumulated for reasons of greed, through criminal activity, and is processed to disguise its illicit origins. Terrorist organizations are motivated by ideology rather than money. While they can be financed through "dirty" money, they can also be financed by money of legitimate origin – from charitable donations, foreign states or even a terrorist's own bank account.

Terrorist financing can involve much smaller sums than are typically involved in money laundering. The money is processed or transferred in ways that seek, not

to disguise its criminal origins, but to disguise its purpose of funding terrorism. Techniques that may work well to identify money laundering, such as a focus on transactions over $10,000, may not work as well to identify those transactions indicative of terrorist financing.

6.4 FINTRAC and its Private Sector Partners

The PCMLTFA requires certain entities ("reporting entities") to report financial transactions to FINTRAC. The ability to add new financial sectors to the list of reporting entities is important since those who finance terrorism will adjust their behaviour to avoid detection through reporting requirements.

FINTRAC's outreach efforts seemed more focused on money laundering than on terrorist financing. FINTRAC should make every effort to provide reporting entities with information that will improve their ability to identify suspicious transactions in terrorist financing matters. When sending information to reporting entities, FINTRAC should prioritize indicators of terrorist financing over indicators of money laundering. In particular, FNTRAC and other authorities should supply up-to-date and user-friendly lists of terrorist entities.

Some reporting entities do not see terrorist financing as a high profile issue. CSIS and the RCMP could help more effectively train reporting entities on terrorist financing issues.

6.5 Information Supplied to FINTRAC Voluntarily by Other Agencies

Information provided voluntarily to FINTRAC by other agencies is vital for FINTRAC's efforts against terrorist financing. About 90 per cent of the terrorist financing cases that come to FINTRAC's attention do so because law enforcement agencies or CSIS have made voluntary reports to FINTRAC. The number of terrorist financing cases discovered solely by FINTRAC is minimal.

A 2008 FATF Mutual Evaluation of Canada (an assessment of Canada's implementation of standards to tackle money laundering and terrorist financing) criticized FINTRAC for excessive reliance on voluntary reports. However, the smaller sums typically at issue in terrorist financing limits the ability of FINTRAC to generate leads on its own.

6.6 Information Sharing

FINTRAC and, to a lesser extent, CRA have an arm's-length relationship with other agencies, particularly law enforcement agencies. There are valid concerns that the police and CSIS may use FINTRAC and the CRA to avoid warrant requirements that would normally apply to obtaining private information. For these reasons, the type of information that FINTRAC or the CRA can disclose to the police or CSIS is closely regulated.

Limits on the information that they can disclose to other agencies, however, should not be confused with limits on the information that FINTRAC and the CRA can receive. FINTRAC, for instance, is required to receive ("shall receive") a broad range of information from other agencies about suspicions of terrorist financing.

One of the dominant themes emerging from the Air India narrative is that agencies all failed to share relevant intelligence, most notably with those who had front-line responsibilities for aviation security. Too often, agencies excessively concerned about protecting information remained isolated in their silos. Every effort should be made to avoid repeating these mistakes in the context of terrorist financing.

The Commission has recommended that the Prime Minister's National Security Advisor be given the added responsibility to work on problems associated with the distribution of intelligence, and to make decisions about what information should be shared, when and with whom. The National Security Advisor could help ensure that intelligence agencies provide FINTRAC and the CRA with relevant information. The National Security Advisor could work on co-ordination issues that are made more difficult when agencies – such as FINTRAC on one hand, and CSIS, the RCMP and the Canada Border Services Agency (CBSA), on the other – fall under different departmental portfolios.

The exchange of information must not be one sided, and it may become necessary to revisit the nature and extent of information that FINTRAC can provide to intelligence and law enforcement agencies. CSIS, CSE, the RCMP, CBSA and CRA must continue to provide FINTRAC with information voluntarily through "Voluntary Information Records" (VIRs). The VIR process is vital to the success of FINTRAC's work on TF. Once it receives a VIR, FINTRAC assesses the information to determine if it can disclose "designated information" to assist the agency that submitted the VIR. However, limits on the types of information that FINTRAC can or must disclose need to be reviewed. For example, a FINTRAC analysis of a particular case cannot be disclosed to another agency unless the agency first obtains a production order. Allowing such disclosures without a production order would add value and context to the financial intelligence that FINTRAC provides.

6.7 Secondments, Joint Training and the Kanishka Centre

An effective approach to terrorist financing would require both increased sharing of information among agencies and increased investment in human capital. One way to achieve the second goal is to facilitate increased secondments among the agencies.

Another is to invest in human capital by providing joint training on terrorist financing across agencies. Joint training might even reduce costs by reducing the duplication of training resources.

Government needs to draw on resources found in the private and academic sectors. One possibility is to provide funding for an academic centre or centres to study terrorism and counterterrorism. A precedent for such a research program exists in the long-running Security and Defence Forum sponsored by the Department of National Defence. The Department funds 12 "centres of expertise" in Canadian universities. Modest sums spent in this way on terrorism and counterterrorism issues could allow the government to receive valuable private sector and academic advice. At the same time, such centres could provide a place for officials to receive training, especially about international best practices. It would be appropriate to name such an institution "the *Kanishka* Centre," to commemorate one of the planes that were targets of the terrorist bombings.

6.8 The Value of Continual Review of the Effectiveness of Anti-terrorism Measures

The National Security Advisor is well positioned to evaluate how FINTRAC works with partners that cross agency lines. One of the enhanced roles recommended for the National Security Advisor is to provide oversight of the effectiveness of national security activities, including those involving terrorist financing. This new role must, however, be exercised reasonably. Too many reviews would monopolize Canadian agencies' resources unnecessarily. A balance is required.

6.9 Charities and Terrorist Financing

The Canada Revenue Agency (CRA) has reported that a significant number of charities associated with terrorism have been denied registered status. Significantly, these denials were not based on the new powers in anti-terrorism legislation but on traditional grounds, not related to terrorism.

The National Security Advisor could also work on problems of integrating the CRA into the intelligence cycle and could also address concerns about the CRA's effectiveness in terrorist financing matters.

The CRA's counter-terrorism work can be assisted by the proposed Director of Terrorism Prosecutions.

The traditional privacy concerns that have surrounded income tax information need to be reconsidered. Bill C-25 started this process. Largely because of provisions introduced by this Bill in 2006, the CRA can now share more information (including "publicly accessible charity information" and "designated taxpayer information") with other agencies. Despite the expanded disclosure now allowed, the *Income Tax Act* still prevents the CRA from disclosing some information that may be relevant to terrorist financing.

6.10 Intermediate Sanctions

"Intermediate sanctions," which are penalties that fall short of revocation of charitable status (for instance, monetary penalties or the suspension of a charity's power to issue tax receipts for donations), can be a valuable tool to alert donors, directors and trustees of government concerned with the operation of a charity. Like targeted prosecutions, they have proven their worth in other jurisdictions as an effective and creative approach to combatting the misuse of charitable status. It is helpful for the CRA to make full use of those intermediate sanctions to encourage charities to "clean house."

6.11 Non-Profit Organizations: A Gap in the System

Although about 95 per cent of the value of donations given to the non-profit sector in Canada goes to registered charities, a small percentage is directed to not-for-profit organizations (NPOs) that do not have charitable status. These organizations can become conduits for terrorist financing because they lack even the modest supervision to which charities are currently subject. Aside from the income tax consequences of having charitable status, the regulation of charities and NPOs is an area of provincial jurisdiction. The evidence before the Commission indicates that provincial regulators are often poorly resourced and not fully aware of relevant information linking NPOs to terrorist financing.

Rules governing NPOs vary among the provinces. In fact, there are few reporting rules in any of the provinces. The problem lies in the ability of NPOs to operate in a clandestine manner and to ignore what rules there are, making it almost impossible to identify terrorist financing within them.

The federal government should take the lead in bringing together provincial authorities to coordinate responses to the abuse of charitable or not-for-profit organizations. It is especially important to ensure that regulators are provided with the information and assistance they need to identify the abuse of charities and not-for-profit organizations for terrorist financing.

VOLUME ONE
THE OVERVIEW

CHAPTER VII: RECOMMENDATIONS AND OBSERVATIONS

Recommendations from VOLUME THREE: The Relationship Between Intelligence and Evidence and the Challenges of Terrorism Prosecution

CHAPTER II: COORDINATING THE INTELLIGENCE/EVIDENCE RELATIONSHIP

Recommendation 1

The role of the National Security Advisor in the Privy Council Office should be enhanced. The National Security Advisor's new responsibilities should be as follows:

- to participate in setting strategic national security policies and priorities;
- to supervise and, where necessary, to coordinate national security activities, including all aspects of the distribution of intelligence to the RCMP and to other government agencies;
- to provide regular briefings to the Prime Minister and, as required, to other ministers;
- to resolve, with finality, disputes among the agencies responsible for national security;
- to provide oversight of the effectiveness of national security activities; and
- to carry out the government's national security policy in the public interest.

In carrying our these new duties, the National Security Advisor should be assisted by a Deputy and by a staff of secondees from agencies which have national security responsibilities, such as CSIS, the RCMP, the CBSA, and DFAIT. The National Security Advisor should continue to support relevant Cabinet committees and serve as Deputy Minister for the CSE, but these duties could, if necessary, be delegated to the Deputy National Security Advisor or to another official within the office of the NSA.

Measures to enhance the role of the NSA should not be delayed until the enactment of legislation on a new national security privilege.

CHAPTER III: COORDINATING TERRORISM PROSECUTIONS

Recommendation 2

The role of the National Security Advisor should be exercised in a manner that is sensitive to the principles of police and prosecutorial independence and discretion, while recognizing the limits of these principles in the prosecution of terrorism offences. The principle of police independence should continue to be qualified by the requirement that an Attorney General consent to the laying of charges for a terrorism offence.

The Attorney General of Canada should continue to be able to receive relevant information from Cabinet colleagues, including the Prime Minister and the National Security Advisor, about the possible national security and foreign policy implications of the exercise of prosecutorial discretion.

Recommendation 3

Terrorism prosecutions at the federal level should be supervised and conducted by a Director of Terrorism Prosecutions appointed by the Attorney General of Canada.

Recommendation 4

The office of the Director should be located within the department of the Attorney General of Canada and not within the Public Prosecution Service of Canada. The placement of the proposed Director of Terrorism Prosecutions in the Attorney General's department is necessary to ensure that terrorism prosecutions are conducted in an integrated manner, given the critical role of the Attorney General of Canada under the national security confidentiality provisions of section 38 of the Canada Evidence Act.

Recommendation 5

The Director of Terrorism Prosecutions should also provide relevant legal advice to Integrated National Security Enforcement Teams and to the RCMP and CSIS with respect to their counterterrorism work to ensure continuity and consistency of legal advice and representation in terrorism investigations and prosecutions.

Recommendation 6

The Director of Terrorism Prosecutions should preferably not provide legal representation to the Government of Canada in any civil litigation that might arise from an ongoing terrorism investigation or prosecution, in order to avoid any possible conflict of interest.

Recommendation 7

A lead federal role in terrorism prosecutions should be maintained because of their national importance and the key role that the Attorney General of Canada will play in most terrorism prosecutions under section 38 of the Canada Evidence Act. The Attorney General of Canada should be prepared to exercise the right under the Security Offences Act to pre-empt or take over provincial terrorism prosecutions if the difficulties of coordinating provincial and federal prosecutorial decision-making appear to be sufficiently great or if a federal prosecution is in the public interest.

Recommendation 8

Provincial Attorneys General should notify the Attorney General of Canada through the proposed federal Director of Terrorism Prosecutions of any potential prosecution that may involve a terrorist group or a terrorist activity, whether or not the offence is prosecuted as a terrorism offence. The National Security Advisor should also be notified.

CHAPTER IV: THE COLLECTION AND RETENTION OF INTELLIGENCE: MODERNIZING THE CSIS ACT

Recommendation 9

In compliance with the 2008 Supreme Court of Canada decision in Charkaoui, CSIS should retain intelligence that has been properly gathered during an investigation of threats to national security under section 12 of the CSIS Act. CSIS should destroy such intelligence after 25 years or a period determined by Parliament, but only if the Director of CSIS certifies that it is no longer relevant.

Recommendation 10

The CSIS Act should be amended to reflect the enhanced role proposed for the National Security Advisor and to provide for greater sharing of information with other agencies.

Section 19(2)(a) of the CSIS Act should be amended to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor.

If the National Security Advisor receives security threat information from CSIS, he or she should have the authority, at any time, to provide the information to the relevant policing or prosecutorial authorities or to other relevant officials with a view to minimizing the terrorist threat. The National Security Advisor should make decisions about whether intelligence should be disclosed only after considering the competing demands for disclosure and secrecy. In every

case, the decision should be made in the public interest, which may differ from the immediate interests of the agencies involved.

Intelligence prepared to assist the National Security Advisor in his or her deliberations, and the deliberations themselves, should be protected by a new national security privilege. The privilege would be a class privilege similar to that protecting information submitted to assist with Cabinet deliberations.

Recommendation 11

To the extent that it is practicable to do so, CSIS should conform to the requirements of the laws relating to evidence and disclosure when conducting its counterterrorism investigations in order to facilitate the use of intelligence in the criminal justice process.

Recommendation 12

In terrorism prosecutions, special advocates, given powers similar to those permitted under the Immigration and Refugee Protection Act, should be allowed to represent the accused in challenging warrants issued under section 21 of the CSIS Act or under Part VI of the Criminal Code. The special advocates should have access to all relevant information, including unedited affidavits used to justify the warrants, but should be prohibited from disclosing this information to anyone without a court order. Both the judges reviewing the validity of warrants and the special advocates should be provided with facilities to protect information that, if disclosed, might harm national security.

CHAPTER V: THE DISCLOSURE AND PRODUCTION OF INTELLIGENCE

Recommendation 13

Federal prosecutorial guidelines should be amended to make it clear to those who prosecute terrorism cases that only material that is relevant to the case and of possible assistance to the accused should be disclosed. Material of limited relevance – in the sense that it is not clearly irrelevant – should, in appropriate cases, be made available for inspection by the defence at a secure location.

Recommendation 14

There is no need for further legislation governing the production for a criminal prosecution of intelligence held by CSIS. The procedures available under section 38 of the Canada Evidence Act provide an appropriate and workable framework for the trial court to determine whether production of such intelligence is warranted.

CHAPTER VI: THE ROLE OF PRIVILEGES IN PREVENTING THE DISCLOSURE OF INTELLIGENCE

Recommendation 15

The RCMP and CSIS should each establish procedures to govern promises of anonymity made to informers. Such procedures should be designed to serve the public interest and should not be focused solely on the mandate of the particular agency.

Recommendation 16

Section 19 of the CSIS Act should be amended to provide that information about an individual which is exchanged by CSIS with a police force or with the NSA does not prejudice claiming informer privilege.

Recommendation 17

CSIS should not be permitted to grant police informer privilege. CSIS informers should be protected by the common law "Wigmore privilege," which requires the court to balance the public interest in disclosure against the public interest in confidentiality. If the handling of a CSIS source is transferred to the RCMP, the source should be eligible to benefit from police informer privilege.

Recommendation 18

The Canada Evidence Act should be amended to create a new national security privilege, patterned on the provision for Cabinet confidences under section 39 of the Act. This new class privilege should apply to documents prepared for the National Security Advisor and to the deliberations of the office of the National Security Advisor.

CHAPTER VII: JUDICIAL PROCEDURES TO OBTAIN NON-DISCLOSURE ORDERS IN INDIVIDUAL CASES

Recommendation 19

The present two-court approach to resolving claims of national security confidentiality under section 38 of the *Canada Evidence Act* should be abandoned for criminal cases. Section 38 should be amended to allow the trial court where terrorism charges are tried to make decisions about national security confidentiality. Section 38 should be amended to include the criminal trial court in the definition of "judge" for the purposes of dealing with a section 38 application that is made during a criminal prosecution.

Recommendation 20

In terrorism prosecutions, there should be no interim appeals or reviews of section 37 or 38 disclosure matters. Appeals of rulings under sections 37 or 38 should not be permitted until after a verdict has been reached. Appeals should be heard by provincial courts of appeal in accordance with the appeal provisions contained in the Criminal Code. If not already in place, arrangements should be made to ensure adequate protection of secret information that provincial courts of appeal may receive. Sections 37.1, 38.08 and 38.09 of the Canada Evidence Act should be amended or repealed accordingly.

Recommendation 21

Security-cleared special advocates should be permitted to protect the accused's interests during section 38 applications, in the same manner as they are used under the Immigration and Refugee Protection Act. Either the accused or the presiding judge should be permitted to request the appointment of a special advocate.

Recommendation 22

The Attorney General of Canada, through the proposed Director of Terrorism Prosecutions, should exercise restraint and independent judgment when making claims under section 38 of the Canada Evidence Act and avoid using overly broad claims of secrecy.

Recommendation 23

The Federal Prosecution Service Deskbook and other policy documents that provide guidance about making secrecy claims should be updated to encourage the making of requests to foreign agencies to lift caveats that they may have placed on the further disclosure of information. These documents should also be updated to reflect the evolution of national security confidentiality jurisprudence. In particular, the Deskbook should direct prosecutors to be prepared to identify the anticipated harms that disclosure would cause, including harms to ongoing investigations, breaches of caveats, jeopardy to sources and the disclosure of secret methods of investigations. The Deskbook should discourage reliance solely on the "mosaic effect" as the basis for making a claim of national security confidentiality.

CHAPTER VIII: MANAGING THE CONSEQUENCES OF DISCLOSURE: WITNESS AND SOURCE PROTECTION

Recommendation 24

A new position, the National Security Witness Protection Coordinator, should be created. The Coordinator would decide witness protection issues in terrorism investigations and prosecutions and administer witness protection in national security matters. The creation of such a position would require amendments to the *Witness Protection Program Act*.

The National Security Witness Protection Coordinator should be independent of the police and prosecution. He or she should be a person who inspires public confidence and who has experience with criminal justice, national security and witness protection matters.

Where appropriate and feasible, the Coordinator should consult any of the following on matters affecting witness and source protection: the RCMP, CSIS, the National Security Advisor, the proposed Director of Terrorism Prosecutors, Public Safety Canada, Immigration Canada, the Department of Foreign Affairs and International Trade and the Correctional Service of Canada. The Coordinator would generally work closely with CSIS and the RCMP to ensure a satisfactory transfer of sources between the two agencies.

The National Security Witness Protection Coordinator's mandate would include:

- assessing the risks to potential protectees resulting from disclosure and prosecutions, as well as making decisions about accepting an individual into the witness protection program and the level of protection required;
- working with relevant federal, provincial, private sector and international partners in providing the form of protection that best satisfies the particular needs and circumstances of protectees;
- ensuring consistency in the handling of sources and resolving disputes between agencies that may arise when negotiating or implementing protection agreements (this function would be performed in consultation with the National Security Advisor);
- providing confidential support, including psychological and legal advice, for protectees as they decide whether to sign protection agreements;
- negotiating protection agreements, including the award of payments;
- providing strategic direction and policy advice on protection matters, including the adequacy of programs involving international co-operation or minors;

- providing for independent and confidential arbitration of disputes that may arise between the protectee and the witness protection program;
- making decisions about ending a person's participation in the program;
- acting as a resource for CSIS, the RCMP, the National Security Advisor and other agencies about the appropriate treatment of sources in terrorism investigations and management of their expectations;
- acting as an advocate for witnesses and sources on policy matters that may affect them and defending the need for witness protection agreements in individual cases.

The National Security Witness Protection Coordinator would not be responsible for providing the actual physical protection. That function would remain with the RCMP or other public or private bodies that provide protection services and that agree to submit to confidential arbitration of disputes by the Coordinator.

CHAPTER IX: MANAGING THE CONSEQUENCES OF DISCLOSURE: THE AIR INDIA TRIAL AND THE MANAGEMENT OF OTHER COMPLEX TERRORISM PROSECUTIONS

Recommendation 25

To make terrorism prosecutions workable, the federal government should share the cost of major trials to ensure proper project management, victim services and adequate funding to attract experienced trial counsel who can make appropriate admissions of fact and exercise their other duties as officers of the court.

Recommendation 26

The trial judge should be appointed as early as possible to manage the trial process, hear most pre-trial motions and make rulings; these rulings should not be subject to appeal before trial.

Recommendation 27

The *Criminal Code* should be amended to ensure that pre-trial rulings by the trial judge continue to apply in the event that the prosecution subsequently ends in a mistrial or is severed into separate prosecutions. The only case in which rulings should not bind both the accused and the Crown should be if there is a demonstration of a material change in circumstances.

Recommendation 28

The *Criminal Code* should be amended to allow omnibus hearings of common pre-trial motions in related but severed prosecutions. This will facilitate severing terrorism prosecutions that have common legal issues where separate trials would be fairer or more manageable. All accused in the related prosecutions should be represented at the omnibus hearing. Decisions made at omnibus hearings should bind the Crown and accused in subsequent trials unless a material change in circumstances can be demonstrated. Such rulings should be subject to appeal only after a verdict.

Recommendation 29

Electronic and staged disclosure should be used in terrorism prosecutions in order to make them more manageable. Disclosure should occur as follows:

Recommendation 30

The Crown should be permitted to provide in electronic form any material on which it intends to rely and should have the discretion to provide paper copies of such material. If the Crown decides to use electronic disclosure, it must ensure that the defence has the necessary technical resources to use the resulting electronic database, including the appropriate software to allow annotation and searching;

Recommendation 31

Material on which the Crown does not intend to rely but which is relevant should be produced in electronic format, and the necessary technical resources should be provided to allow the use of the resulting electronic database;

Recommendation 32

The Crown should be able to disclose all other material that must be disclosed pursuant to *Stinchcombe* and *Charkaoui* by making it available to counsel for the accused for manual inspection. In cases where the disclosure involves sensitive material, the Crown should be able to require counsel for the accused to inspect the documents at a secure location with adequate provisions for maintaining the confidentiality of the lawyer's work. Defence counsel should have a right to copy information but subject to complying with conditions to safeguard the information and to ensure that it is not used for improper purposes not connected with the trial;

Recommendation 33

The trial judge should have the discretion to order full or partial paper disclosure where the interests of justice require; and

Recommendation 34

The authority and procedures for electronic disclosure should be set out in the *Criminal Code* in order to prevent disputes about electronic disclosure.

Recommendation 35

It is recommended that:

a) the *Criminal Code* be amended to allow the judge in a jury trial to empanel up to 16 jurors to hear the case if the judge considers it to be in the interests of justice;

b) if more than 12 jurors remain at the start of jury deliberations, the 12 jurors who will deliberate be chosen by ballot of all the jurors who have heard the case;

c) the minimum number of jurors required to deliberate remain at 10;

d) the idea of having terrorism trials heard by a panel of three judges be rejected because it offers no demonstrable benefit; and

e) the call for mandatory jury trials in terrorism cases be rejected in view of the difficulties of long trials with juries and the accused's present ability to opt for trial by judge alone.

Recommendations from VOLUME FOUR: Aviation Security

CHAPTER IV: RECOMMENDATIONS

I. Oversight of Aviation Security in Canada

The Commission endorses the Government's decision that responsibility for national civil aviation security should remain with Transport Canada, and makes the following recommendations about oversight of aviation security:

Recommendation 1

1. Canada's regulatory regime must comply with the standards specified in Annex 17 to the Convention on International Civil Aviation ("Chicago Convention") and should comply with its recommended practices.

   1.1 Annex 17 standards must be considered minimum standards that Canada should not only meet, but exceed. Canada should not permit security deficiencies that would result in it being required to file a difference with the International Civil Aviation Organization (ICAO) with respect to any Annex 17 standard.

1.2 In addition to embracing Annex 17 at its core, Canada's national regulatory regime must be informed by international best practices and must address Canada's unique threat environment.

1.3 Transport Canada should exercise robust regulatory oversight over civil aviation stakeholders through regular inspection, testing, auditing and enforcement, carried out by a sufficiently trained, qualified and resourced inspectorate.

Recommendation 2

2. In accordance with Annex 17, Transport Canada should establish and implement a single, written National Civil Aviation Security Program that comprehensively safeguards civil aviation against acts of unlawful interference.

2.1 The National Civil Aviation Security Program should set out the full slate of legislative instruments, measures, policies, practices and procedures, as well as the roles and responsibilities of Transport Canada, airport operators, air carriers, Fixed Base Operations (FBOs), the General Aviation (GA) sector, the Canadian Air Transport Security Authority (CATSA), the police of local jurisdiction, airport tenants, caterers and all other entities involved in implementing the Program.

2.2 Transport Canada should require all entities with responsibilities in civil aviation security, as outlined in Recommendation 2.1, to establish and implement written security programs that are applicable to their operations and appropriate to meet the requirements of the National Civil Aviation Security Program. At a minimum, these programs should include measures to prevent unauthorized access, assign security-related duties, respond to threats and breaches of security, and allow for periodic review and updating of the programs.

2.3 Transport Canada should require all civil aviation stakeholder programs to be submitted to it for approval.

Recommendation 3

3. The Commission supports continued coordination between all industry and government entities responsible for civil aviation security through the Advisory Group on Aviation Security (AGAS). AGAS must continue to promote collaboration, shared objectives and shared understanding, and common solutions to aviation security problems.

3.1 Transport Canada should require all airports to establish an airport security committee to help in implementing their respective airport security programs.

3.2 Consideration should be given to the inclusion of the National Security Advisor (NSA) in AGAS discussions and decisions.

Recommendation 4

4. In addition to adhering to Annex 17 standards, a regulatory regime should observe a number of key principles:

a. Ongoing, informed assessment of past, present and future threats to civil aviation, with timely proactive adjustments made to the regime as needed;

b. Adherence to an appropriate national risk management protocol, as described in Recommendation 6;

c. Effective, multi-layered and overlapping security measures, policies, practices and procedures that provide redundancies to address all significant risks;

d. A flexible, performance-based approach to regulation, in which objectives are set to meet the highest standards, with a more prescriptive approach employed where necessary because of complexities and context;

e. Robust emergency response planning, with well-defined roles and responsibilities; and

f. Establishment of a culture of security awareness and constant vigilance.

Recommendation 5

5. Independent experts should conduct a comprehensive review of aviation security every five years.

II. Risk Management

Recommendation 6

6. Transport Canada should ensure that acceptable levels of risk control have been achieved in all areas of risk pertinent to civil aviation security in Canada. In doing so, it should adopt a national risk management protocol based on best practices and using a performance standard of continuous improvement, delivering levels of risk in all relevant areas that are as low as reasonably achievable. Where acceptable levels have not been achieved, resources must be allocated on a priority basis to address the risk appropriately.

6.1 To facilitate clear communication and understanding, Transport Canada should require those responsible for aviation security to follow a common set of risk management protocols consistent with the national protocol. Transport Canada should require all stakeholders to:

a. Provide a detailed description, in their respective security programs that are submitted to Transport Canada for acceptance or approval, of the risk management protocol employed for their operations;

b. Systematically employ these risk management protocols in the development and implementation of aviation security measures, policies, practices and procedures for their operations; and

c. Promote coordinated risk management decision-making by engaging in ongoing dialogue with Transport Canada and other stakeholders through participation in AGAS and its technical committees, and elsewhere as necessary, to ensure clarity, precision and a shared understanding of terminology and methodologies.

6.2 Each year, the Minister of Transport should certify that the civil aviation security regime in Canada possesses:

a. A common set of protocols for carrying out risk management, based on current best practices;

b. A performance standard of continuous improvement, delivering levels of risk in all relevant areas that are as low as reasonably achievable; and

c. Acceptable levels of risk control in all domains of risk.

6.3 Periodic assessment of Transport Canada's risk management protocol by the Auditor General is encouraged.

Recommendation 7

7. There should be no significant gaps in civil aviation security. When a significant deficiency is identified, the best interim measures must be implemented to address the risk while more permanent measures, including technological solutions, are developed.

7.1 The civil aviation security regime must be capable of redeploying resources so that all significant threats are adequately addressed and measures do not disproportionately emphasize a particular threat, such as the threat posed by passengers and baggage.

7.2 As soon as improved equipment and measures become available, they should be deployed.

7.3 If, after a systematic risk management process, a decision is made not to implement measures that address a given threat, measures should nonetheless be designed for emergency implementation if the threat subsequently becomes imminent.

7.4 Legislative initiatives to improve civil aviation security should not be subject to unreasonable delay.

Recommendation 8

1. Transport Canada and others responsible for civil aviation security should foster a culture of security awareness and constant vigilance. As part of this endeavour, a comprehensive public education campaign should be developed to increase awareness of the measures in place for the public's protection and the role the public can play in promoting security.

III. Use of Intelligence

Recommendation 9

9. Transport Canada must provide timely, relevant and actionable intelligence information to civil aviation stakeholders, with the primary recipients being airport operators, air carriers, pilots, CATSA, FBOs and GA facilities.

9.1 Transport Canada should be guided by the "need to share" principle and should cooperate more closely with key stakeholders to ensure they receive the intelligence information they require.

9.2 Aviation stakeholders should provide Transport Canada with feedback about the quality and timeliness of intelligence they receive. Where concerns are raised, a collaborative approach to resolving those concerns should be taken.

9.3 In addition to threats related to airports and air carriers, aviation stakeholders should be kept abreast of changes to the general threat environment. Regular security briefings for all stakeholders, including front-line workers, should occur.

IV. Airport Security

Recommendation 10

10. Non-Passenger Screening (NPS) should be improved at all designated airports in Canada on a priority basis.

10.1 Full (100 per cent) NPS should be implemented upon entry to restricted areas at all Class 1 and Class 2 airports, with random NPS upon exit at Class 1 airports.

10.2 NPS upon entry at Class Other and upon exit at Class 2 and Class Other airports should be implemented as necessary, based on risk.

Recommendation 11

11. Perimeter security should be improved at all designated airports on a priority basis.

11.1 Perimeter security should be enhanced with physical and technological barriers and appropriate monitoring, based on risk.

11.2 Transport Canada should conduct intrusion tests of airport perimeters.

Recommendation 12

12. All vehicles entering airside and restricted areas at Class 1 airports should be subject to a full search, including full NPS of occupants. Vehicles entering Class 2 airports should be searched as necessary, based on risk.

12.1 Where supply chain security measures have been applied to vehicles, a search may be confined to the areas of the vehicle that have not been secured, and should include full NPS of occupants.

12.2 CATSA's mandate should be expanded on a priority basis to include searching vehicles and screening their occupants. CATSA should be provided with the necessary funding.

Recommendation 13

13. The Restricted Area Identification Card (RAIC) should be implemented at all 89 designated airports on a priority basis, and should be expanded to include perimeter security, including vehicle gates, FBOs and tenant facilities.

13.1 RAICs, Restricted Area Passes (RAPs) and temporary or visitor passes should be worn and clearly displayed at all times by all individuals who access restricted and airside areas of the airport.

13.2 All access control devices, including RAICs and RAPs, should be implemented in a manner that prevents "piggybacking," "tailgating" and other means of gaining unauthorized access.

13.3 All RAICs and RAPs, as well as employee uniforms and any other form of airport identification belonging to former airport employees, should be diligently accounted for, retrieved and/or deactivated. Appropriate penalties should be imposed for failing to return such items.

Recommendation 14

14. For FBOs and GA facilities attached to designated airports, access to the airports' airside and restricted areas should be strictly controlled through RAICs, full NPS and vehicle searches.

Recommendation 15

15. Transport Canada should improve its policies and procedures governing transportation security clearances.

15.1 Transport Canada and the RCMP should increase efforts to share information on individuals applying for a transportation security clearance to work at airports.

15.2 Transport Canada should establish a formal process, including specific criteria, for reviewing applications for security clearances made by individuals with a criminal record.

15.3 Transport Canada should reinstate credit checks as a component of the security clearance process before issuing an RAIC for non-passengers who require access to restricted areas at airports.

15.4 Transport Canada should take steps to reduce the delay in processing applications for transportation security clearances.

Recommendation 16

16. Security measures should be developed and implemented to protect public areas of air terminal buildings at Class 1 airports, based on risk.

Recommendation 17

17. All airports should develop and implement a security awareness and constant vigilance program that includes training for all airport workers employed in air terminal buildings and airside portions of airports.

V. Passenger and Baggage Screening

Recommendation 18

18. Current methods for conducting pre-board screening (PBS) are comprehensive, but improvements are required in their application.

18.1 Although technology has enhanced the ability to effectively conduct PBS, that technology should rarely be relied upon exclusively.

When selecting equipment and procedures for passenger screening, consideration should be given to individual rights, including privacy rights and the rights guaranteed under the *Canadian Charter of Rights and Freedoms*. In particular, any consideration of behavioural analysis techniques as a tool for PBS must include a thorough review. Concerns about the risk of racial, ethnic and religious profiling must be given specific and careful attention. If a decision is made to implement such a program, the following must be addressed: effectiveness of the measure; competencies, training (initial and ongoing) and testing required of those who would conduct the analysis; and oversight requirements.

18.2 Given the importance of the "no search, no fly" rule and the potential impact of security measures on individual rights, Transport Canada and the Office of the Privacy Commissioner of Canada should collaborate to devise tools and criteria to evaluate proposed security measures.

Recommendation 19

19. Although the multi-level system in place for Hold Bag Screening (HBS) is comprehensive, some improvements are required.

19.1 Baggage should never be loaded onto an aircraft without a passenger-baggage reconciliation. Interlined baggage, in particular, must be subjected to comprehensive passenger-baggage reconciliation prior to being loaded.

19.2 Consideration should be given to whether the current administrative monetary penalties for non-compliance with passenger-baggage reconciliation procedures provide sufficient deterrence and reflect the gravity of the potential consequences of non-compliance.

19.3 Although technology has enhanced the ability to effectively screen checked baggage, that technology should rarely be relied upon exclusively.

VI. Use of Technology and Explosives Detection Dogs

Recommendation 20

20. Transport Canada should ensure that all screening technology is reliable and effective. This requires assessment not only during the development and deployment stages, but also continual assessment during conditions of actual use.

20.1 Transport Canada should ensure that screening officers operating equipment are adequately trained and regularly tested to ensure their competence.

20.2 Transport Canada should ensure that screening equipment is properly maintained.

Recommendation 21

21. The use of explosives detection dogs should be evaluated and expanded as appropriate. Consideration should be given to their use in:

a. PBS and HBS;
b. Screening of air cargo; and
c. Perimeter security, including the screening of vehicles.

VII. Screeners

Recommendation 22

22. CATSA should find long-lasting solutions to resolve difficulties in the recruitment of appropriately qualified screening contractors and in the recruitment, retention, training and oversight of competent screening officers to ensure the highest quality of screening.

22.1 Because of the voluminous material that all screening officers are required to master, consideration should be given to specifying a minimum educational requirement for them in the *Designation Standards for Screening Officers*.

22.2 Given the importance of their work, screening officers should receive appropriate compensation and employee benefits to reduce difficulties in retaining them.

22.3 Because of the challenges associated with their duties, particularly repetitive, stressful and monotonous work that only rarely results in finding prohibited items, CATSA should make ongoing efforts to instill greater sense of mission and morale among screening officers:

a. Consideration should be given to creating an employment structure that provides opportunities for advancement; and

b. Consideration should be given to holding regular briefings for screening officers, particularly at Class 1 airports, to provide relevant intelligence updates, as well as information relating to prohibited items, methods of concealment and information contained in recent Transport Canada bulletins.

22.4 Screening officer duties should focus solely on preventing unlawful interference with civil aviation. Screening officers should not be mandated to search for contraband or other items that may interest law enforcement, but that are not relevant to CATSA's mandate.

22.5 Given the changing nature of threats to aviation, training of screening officers should be continuous. Training should include instruction in practical skills and in the detection of improvised explosive devices (IEDs).

22.6 Training of screening officers should be designed to foster a general culture of security awareness and constant vigilance.

22.7 CATSA should continue to use training and motivational tools such as X-ray Tutor (XRT) and the Threat Image Projection System (TIPS).

22.8 Where screening officer deficiencies are identified, immediate steps, primarily additional training, should be taken to ensure competence.

22.9 Transport Canada should define clear and consistent system-wide performance standards for CATSA, in addition to the failure rate for infiltration tests, against which compliance and effectiveness can be assessed. Performance measures should define whether CATSA's performance is satisfactory or unsatisfactory:

a. This should include agreement between Transport Canada and CATSA regarding the threshold for failure of infiltration tests and the specific elements that constitute failure; and

b. CATSA's response to failed infiltration tests should emphasize re-training, and should include documentation of corrective action taken and timely written responses to Transport Canada enforcement letters and related enquiries.

22.10 Whenever the Auditor General of Canada deems it necessary, the Auditor General should review the changes implemented by CATSA to address problems with recruitment, retention, training, testing and oversight of screening officers.

VIII. Air Cargo and Other Non-Passenger Items

Recommendation 23

23. A comprehensive system for screening air cargo (including mail) for transport on passenger and all-cargo aircraft should be implemented as an urgent priority. Canada's system of Known Shippers should be discontinued as soon as possible, and a system of Regulated Agents put in its place in accordance with international best practices. In designing and implementing the system, the Government should exceed the minimum requirements of Annex 17 of the *Chicago Convention*, with the aim of achieving the highest possible standards of air cargo security.

23.1 The Commission supports Transport Canada's proposed Air Cargo Security (ACS) Initiative and recommends its implementation on a priority basis.

23.2 Under the new regime, all air cargo to be loaded onto passenger aircraft should be screened to a level comparable to that currently provided for hold baggage.

23.3 All air cargo to be loaded onto all-cargo aircraft should be screened to a level deemed appropriate, on the basis of risk. When air cargo is

transferred from all-cargo to passenger aircraft, additional screening should be conducted commensurate with screening requirements that normally apply to air cargo carried on passenger aircraft.

23.4 Screening for air cargo should take into account the risk posed by new, emerging or otherwise unaddressed threats as they arise.

23.5 The evaluation of technologies to screen consolidated or bulk cargo should be accelerated.

23.6 A centralized screening service for all air cargo requiring screening at the airport should be considered for all Class 1 airports.

23.7 CATSA, with its screening mandate, expertise, equipment and dedicated personnel, is the appropriate authority to conduct air cargo screening services at the airport and may have a role to play in the oversight and inspection of screening by Regulated Agents. CATSA's mandate should be expanded by legislation to include the screening of air cargo.

23.8 Care must be taken to provide adequate training for all air cargo screeners. This should include rigorous testing for required competencies. The development and implementation of computer software training and screening aids should be accelerated.

23.9 Transport Canada should employ a sufficient number of security inspectors trained and qualified for inspecting, testing, auditing and enforcing the new air cargo security regime.

23.10 Funding for the ACS Initiative must ensure that it remains sustainable and can respond to emerging or otherwise unaddressed threats.

23.11 Annual progress reports on enhancements in air cargo security should be provided to Parliament by the Minister of Transport for each of the five years following release of the Commission's report.

Recommendation 24

24. The new security regime for air cargo must be governed by legislation, not by non-binding Memoranda of Understanding. The security regime should reflect international best practices.

24.1 Legislative provisions should include, but not be limited to, the following:

a. Mandatory security programs for all Regulated Agents, with formal approval from Transport Canada;

b. Clear definitions for terminology, including the terms "screen," "inspect" and "search";

c. Measures and technologies for screening air cargo;

d. Screening requirements for all Regulated Agents, whether shippers, freight forwarders or air carriers;

e. Appropriate training requirements for all Regulated Agents, their employees and sub-contractors;

f. Requirements to maintain the security of off-airport premises to a specified level wherever cargo is handled, stored and potentially accessed;

g. Requirements to maintain the security of off-airport vehicles to a specified level for the transport of air cargo to its final point of transfer;

h. Requirements for ensuring appropriate access and security controls for air cargo while on airport premises, during transfer to the aircraft and on loading onto the aircraft;

i. Mandatory security clearances, including a credit check, for all workers who have access or potential access to air cargo from the point of receipt to the point of transfer, including sub-contractors engaged to handle cargo on behalf of a Regulated Agent;

j. A system of inspection, testing, auditing and enforcement by Transport Canada or its designated agent; and

k. Methods of enforcement, including administrative monetary penalties and other penalties that reflect the potential gravity of the consequences of non-compliance.

24.2 Regulated Agent security programs should describe all measures, practices, policies and procedures applicable to air cargo security that have been, or will be, implemented by the Regulated Agent, including security awareness programs and risk management protocols.

Recommendation 25

25. A supply chain security regime should be established for other non-passenger items (such as stores and catering) that are prepared at off-airport premises before being delivered to an aircraft.

IX. Fixed Base Operations and General Aviation

Recommendation 26

26. As an urgent priority, all passengers and carry-on and checked baggage boarding flights at FBOs and GA facilities that feed into designated airports or are attached to designated airports should be screened to a level comparable to passenger and baggage screening for scheduled commercial flights.

26.1 As an equally urgent priority, all non-passengers entering such FBO and GA facilities should be screened to an acceptable level, based on appropriate risk management protocols;

26.2 All non-passenger items (including air cargo) to be placed on flights departing from such FBO and GA facilities should be screened to an acceptable level, based on appropriate risk management protocols.

26.3 On a priority basis, all FBO and GA facilities should develop and implement a security awareness and constant vigilance program that supports a "neighbourhood watch" approach to security. An accompanying training program should be developed and implemented for all personnel to foster a culture of security awareness and constant vigilance.

26.4 CATSA should oversee security screening services at FBOs and GA facilities. If CATSA's resources are engaged, additional government funding should be provided.

26.5 The aviation security requirements for FBOs and GA facilities should be governed by legislation.

XI. Duty to Warn and Transparency

Recommendation 27

27. The development of a public warning system for threats against airlines should receive further study. Issues include:

a. international experience with such systems;

b. the circumstances under which public warnings of threats have occurred in Canada;

c. the proper balance between security and industry interests;

d. the proper balance between the need for secrecy and the need to instill public confidence;

e. the appropriate threshold at which a public warning should be issued; and

f. the policy and legal implications, including possible liability to air carriers whose operations could be compromised by a public warning.

Recommendation 28

28. In general, greater transparency in aviation security is required to inspire confidence in the system, to provide assurance that resources are effectively allocated and to ensure that government and industry stakeholders remain accountable for managing this mandate.

28.1 The Commission does not recommend publishing intrusion test results. If a decision is nonetheless made to publish them, publication should only occur after enough time has passed to enable vulnerabilities identified by the tests to be addressed.

XII. Funding

Recommendation 29

29. As a core mandate directly related to national security, civil aviation security should receive sustained funding, regardless of prevailing economic circumstances, to maintain an acceptable level of security.

29.1 Funding for civil aviation security should be derived primarily from government.

29.2 Funding priorities should be directed to areas of risk that have not achieved an acceptable level of risk control, such as air cargo and control of access to airside and restricted areas of airports.

29.3 If additional funds are required for initiatives related to passenger and baggage security, the Commission supports the continuance of an Air Travellers Security Charge (ATSC). However:

a. The collection, retention and disbursement of the ATSC should be subjected to comprehensive and transparent accounting. All revenue from the ATSC should be traceable and should be used solely for civil aviation security;

b. An annual report of ATSC revenues as well as expenditures by program or department is recommended; and

c. CATSA should be the main beneficiary of funds from the ATSC.

Observations

1. In light of all the evidence before it, the Commission believes that the RCMP is not properly structured to deal with the unique challenges of terrorism investigations. There is merit in considering structural changes to allow for a greater degree of specialization and for a more concentrated focus on investigating and supporting the prosecution of national security offences. This may mean divesting the RCMP of its contract policing duties so as to simplify lines of communication and to clarify the national dimensions of its mandate as a pan-Canadian police force.

2. The funding of an academic institute for the study of terrorism – possibly to be called the "Kanishka Centre" to commemorate the name of the aircraft that was bombed on June 23, 1985 – could be an important step toward preventing future terrorist attacks while honouring the memory of those who perished.

3. The Commission believes that there would be great merit in a demonstration of solicitude by the present Government for the families of the victims of the bombing. To that end, an independent body should be created to recommend an appropriate *ex gratia* payment and to oversee its distribution.

4. At an appropriate time the Government should provide a report detailing which recommendations of the Commission have been implemented, and which have been rejected or are subject to further study.

Volume One
The Overview

Annexes

ANNEX A: COMMISSION RULINGS

RULING ON STANDING AUGUST 9, 2006
REASONS FOR RULINGS ON STANDING

1. INTRODUCTION

I received 21 applications for standing from groups or individuals. I have given each application due consideration and have appended to these Reasons the consequent ruling for each applicant.

Before I turn to a discussion of the merits of each application, I will review some of the principles and rules that have guided my decisions on standing.

2. GUIDING PRINCIPLES ON STANDING

The Terms of Reference and draft Rules of Procedure and Practice contemplate two types of standing in this Inquiry: that of parties and that of intervenors.

The Terms of Reference establishing this Inquiry give the Commissioner the authority:

...to grant to the families of the victims of the Air India Flight 182 bombing an opportunity for appropriate participation in the Inquiry; and

...to grant to any other person who satisfies him that he or she has a substantial and direct interest in the subject-matter of the Inquiry an opportunity for appropriate participation in the Inquiry.

The Terms of Reference also authorize the Commissioner:

...to adopt any procedures and methods that he may consider expedient for the proper conduct of the Inquiry...

Pursuant to this latter authority, draft Rules of Procedure and Practice (the "Rules") have been issued.

Rule 10 provides:

A person may be granted full or partial standing as a party by the Commissioner if the Commissioner is satisfied that the person is directly and substantially affected by the mandate of the Inquiry or portions thereof.

Therefore, aside from family members and associations of family members who presumptively, pursuant to paragraph (f) of the Terms of Reference, have the requisite interest in participation in this Inquiry, other groups or individuals must demonstrate a direct and substantial interest before party standing will be granted.

Justice John Gomery, in his reasons with respect to standing before the Commission of Inquiry into the Sponsorship Program and Advertising Activities, explained the concept of "substantial and direct" interest as follows:

What constitutes a "substantial and direct interest in the subject matter of the Inquiry"? Based upon what has been decided in comparable cases, the interest of the applicant may be the protection of a legal interest in the sense that the outcome of the Inquiry may affect the legal status or property interests of the applicant, or it may be as insubstantial as the applicant's sense of well-being or fear of an adverse effect upon his or her reputation. Even if such a fear proves to be unfounded, it may be serious and objectively reasonable enough to warrant party or intervenor standing in the Inquiry. What does not constitute a valid reason for a participant's standing is mere concern about the issues to be examined, if the concern is not based upon the possible consequences to the personal interests of the person expressing the concern. As was stated by Campbell J. in *Range Representative on Administrative Segregation Kingston Penitentiary v. Ontario* (1989), 39 Admin. L.R. at p. 13, dealing with a coroner's inquest:

Mere concern about the issues to be canvassed at the inquest, however deep and genuine, is not enough to constitute direct and substantial interest. Neither is expertise in the subject matter of the inquest or the particular issues of fact that will arise. It is not enough that an individual has a useful perspective that might assist the coroner.

Therefore, while the test for "substantial and direct" interest is not precise, applicants must in some way be *directly* affected by the conclusions reached in the Inquiry to be granted party standing.

However, the success of this Inquiry is also dependent on the participation of those individuals, groups and organizations that, while not affected directly by the mandate, can provide crucial perspectives in relation to the Terms of Reference.

In this regard, Rule 11 provides:

A person may be granted standing as an intervenor by the Commissioner if the Commissioner is satisfied that the person represents clearly ascertainable interests and perspectives essential to the Commissioner's mandate, which the Commissioner considers ought to be separately represented before the Inquiry, in which event the intervenor may participate in a manner to be determined by the Commissioner.

Insofar as the Terms of Reference touch on issues that may affect or engage certain segments of Canadian society in unique and important ways, I should hear these voices and perspectives.

However, my mandate and role must at all times be guided by the Terms of Reference and the Rules, and it is in the public interest that this Inquiry be focused

and conducted as expeditiously as possible. Therefore, I cannot grant intervenor status unless applicants have ascertainable interests and perspectives that are *essential* to my mandate. It is not enough that an individual or organization has interests that overlap with the Inquiry or the desire to influence its outcome. With these principles in mind, I now turn to my findings.

3. DISPOSITIONS

These applications can conveniently be broken out into a number of categories:

1) Family members and associations of family members

I received applications from the following groups representing family members of the victims of the bombing:

- Air India Cabin Crew Association (AICCA)
- Air India Victims Families Association (AIVFA)
- Family members of the crew member victims of Air India Flight 182, and India nationals (FMCMV/IN)
- I also received applications from the following individuals who are family members:
- Mr. Sanjay Lazar
- Ms. Lata Pada
- Mr. Niraj Sinha

During the course of the hearing, I was advised that AICCA and FMCMV/IN intend to join forces and collaborate with each other, and that Mr. Lazar intends to join that group as well.

AIVFA stated that it represents a large proportion of family members residing in North America, and is still gathering new applications for membership.

Ms. Pada stated that she is working with a number of family members residing in North America who are not members of AIVFA.

Mr. Sinha resides in India and has applied in writing.

All of the foregoing individuals and groups are entitled to participate pursuant to paragraph (f) of the Terms of Reference. They all have a direct and substantial interest in the subject matter of the Inquiry within the meaning of Rule 10 and should therefore be granted party status.

I find that the appropriate level of participation of these groups and individuals can be achieved on the following terms:

AICCA, FMCMV/IN, Mr. Lazar and Mr. Sinha all are or represent family members or groups of family members of victims of the bombing who reside in India or elsewhere outside of North America. They form a natural grouping for the purposes of representation.

AIVFA represents a large and potentially growing number of family members of victims of the bombing who reside in North America. It forms a natural group for the purposes of representation.

Ms. Pada and other individuals who did not apply separately but are aligned with her form a natural grouping for the purposes of representation.
Each of the preceding three groups of family members should be granted status as parties for the purposes of participation in this Inquiry pursuant to the Rules.

Proper conduct of the Inquiry requires that repetition be minimized to the extent possible. Each group is therefore encouraged to cooperate and collaborate with other groups to the extent possible, and is expected to avoid repetition in its participation.

On that basis, party status is granted on the terms set out in the rulings attached to these reasons.

2) Government of Canada

The Department of Justice acts for the departments and agencies of the Government of Canada, as well as for the Government itself. The departments and agencies relevant to the Inquiry include: RCMP, CSIS, Transport Canada, FINTRAC, Communications Security Establishment, Department of Foreign Affairs and International Trade, Department of Finance, and Canada Revenue Agency. Counsel for the Department of Justice indicated at the hearing that the Department of Justice had canvassed the issue of conflict and will address any conflict, should it arise, to ensure that there is no interruption in the proceedings of the Inquiry. The Government of Canada will "attempt to speak with one voice."

Departments and agencies of the Government of Canada clearly have a substantial and direct interest in the subject matter of the Inquiry. The conclusions of this Commission will have direct implications for their policies, legislation, protocols and activities. In addition, the historical portion of the mandate directly implicates a number of specific departments and agencies. The Attorney General of Canada should be granted status as a party to participate on the Government's behalf pursuant to the Rules.

3) Air India

Air India applied for standing as a party to participate in the Inquiry with respect to subparagraphs (b)(i), (ii), (iv), (vi) and (vii) of the Terms of Reference.

As set out in its application, Air India clearly has a substantial and direct interest in the subject matter of the Inquiry. It should therefore be given status as a party to participate, as set out in the Rules, with respect to those parts of the mandate of the Inquiry.

4) Groups, associations and organizations claiming special expertise with respect to all or part of the mandate of the inquiry

The following groups, associations and organizations provided affidavit evidence as to their experience and expertise with respect to all or part of the mandate of the Inquiry:

- B'nai Brith Canada
- Canadian Civil Liberties Association (CCLA)
- Canadian Coalition Against Terror (C-CAT)
- Canadian Coalition for Democracies (CCD)
- Canadian Council on American Islamic Relations and Canadian Muslim Civil Liberties Association (CAIR-CAN/CMCLA)
- Canadian Jewish Congress (CJC)
- Canadian Resource Centre for Victims of Crime (CRCVC)
- World Sikh Organization of Canada (WSO)

On examination of the evidence, it is my view that none is affected in such a direct and substantial manner so as to qualify as a party pursuant to Rule 10, but that each qualifies, pursuant to the test set out in Rule 11, for participation as an intervenor.

I find that the proper conduct of the Inquiry requires that in each case the participation of the intervenor should be limited to areas of demonstrated experience and expertise. On the basis of the affidavit evidence, the proper scope of participation for each of the intervenors is that set out in the rulings appended hereto.

I find further that, pursuant to paragraph (d) of the Terms of Reference and pursuant to Rule 11 of the draft Rules, the proper conduct of the Inquiry will be facilitated by restricting the participation of each intervenor at first instance to written submissions with respect to the areas of the Inquiry or portions of the mandate for which they were granted standing.

Individual intervenors may wish to extend their participation beyond written submissions. Different applicants in this group asked for specific extended rights of participation. Once they file their written submissions, intervenors are at liberty to apply for extended rights of participation, including the right to make a 10-minute opening statement, or other participation as envisaged by the Rules. Such applications should be made in writing, addressed to Commis-

sion Counsel, with a copy to the Registrar. I shall deal with each such application on the merits, subject to such additional process, if any, as will be determined at the time of application.

The Canadian Bar Association (CBA) applied in writing and asked for leave to extend the time to apply for standing as an intervenor. I hereby grant such leave, and upon review of the CBA's materials, also grant the CBA intervenor status in accordance with the terms set out above and with the rulings appended hereto.

5) Mr. Ripudaman Singh Malik

Mr. Malik was charged in connection with the bombing of Air India Flight 182. He was acquitted in proceedings reported as *R. v. Malik*, [2005] B.C.J. No. 521 (B.C.S.C.). Mr. Malik applied in writing for standing with respect to the mandate of the Inquiry.

Paragraph (p) of the Terms of Reference prohibits the Commissioner from "expressing any conclusion or recommendation regarding the civil or criminal liability of any person or organization." Mr. Malik has a substantial and direct interest in a finding regarding his civil or criminal liability or lack thereof with respect to the bombing, but that is not part of the mandate of the Inquiry. While Mr. Malik may have personal experience or evidence as to the impact on him of any alleged deficiencies in the conduct of the investigation into the bombing and of the conduct of the trial, such experience does not vest him with the special expertise with respect to the specific issues within the mandate of the Inquiry and about which I am to report.

Mr. Malik's affidavit focuses largely on his interests in his reputation and on the possibilities he perceives for damage to those interests during the course of the Inquiry. In view of paragraph (p) of the Terms of Reference, there should be little if any relevant evidence that could have the impact on Mr. Malik's interests in his reputation that he fears. Nevertheless, a possibility does exist of such negative impact, and in light of the possibility, I find that Mr. Malik has, to that extent, an interest in the subject matter of the Inquiry, limited as that interest may be.

I find that, pursuant to Rule 11, the appropriate standing for Mr. Malik is as an intervenor, and that his interest in the subject matter of the Inquiry can be accommodated at first instance by participation in writing.
As with other intervenors, Mr. Malik is at liberty to apply in writing for expanded participation. The same rules that apply to the other intervenors should apply to Mr. Malik in this regard.

6) Other individuals who applied for standing

Mr. John Barry Smith, Mr. Arnold Guetta and Mr. Thomas Quiggin also applied for standing.

I find that, as interesting as the perspectives of these individuals may be, their experience and perspectives are not directly applicable to the mandate of the Inquiry, nor are their specific interests directly and substantially affected by the mandate. Accordingly, these individuals should be denied standing. Having regard, however, to the effort they have expended in preparing materials, they should be at liberty to file written materials with the Inquiry. They are to have no additional rights or status.

RULING ON STANDING
August 23, 2006
(Criminal Lawyers' Association - CLA)

Request by Applicant

CLA applied in writing and asked for leave to extend the time to apply for standing before the Inquiry. CLA sought full party status at Stage 2 of the Inquiry. In the alternative, CLA sought partial party status with respect to Terms of Reference b)iii), b)v) or b)vi). In the further alternative, CLA sought intervenor status with respect to Terms of Reference b)iii), b)v) or b)vi).

Disposition

Leave to extend the time to apply for standing is granted, and **intervenor** status is granted on the following basis:

CLA is granted the right, in the first instance, to provide written submissions with respect to Terms of Reference b)iii), b)v), and b)vi), especially as they relate to issues of how changes to the traditional criminal law model are likely to impact on defence lawyers' ability to discharge their public duty of testing the reliability of evidence in the context of terrorism cases.

Rules Applicable to All Intervenors

The following rules apply to all intervenors who wish to apply for leave to assume a broader role beyond the filing of written submissions:

Following the filing of their written submissions, intervenors may apply for leave to make a 10 minute opening statement.

Any intervenor wishing to propose a witness to be called by Commission Counsel may make submissions in writing, with reference to Rules of Procedure and Practice 44 and 49, outlining the nature and importance of the anticipated evidence to be given by such witness.

Any intervenor wishing to participate in a manner beyond that envisioned in paragraphs 1 and 2 above, may apply in writing for leave, outlining the nature of the proposed additional participation and attaching submissions as to the unique and valuable contribution to the accomplishment of the mandate of the Commission that would result from such additional participation.

All written submissions and applications are to be submitted in hard copy to Commission Counsel at the address of the Commission, with a copy to the Registrar.

RULING ON STANDING
November 1, 2006
(Canadian Association of Chiefs of Police - CACP)

Request by Applicant

CACP applied in writing and asked for leave to extend the time to apply for standing before the Inquiry. CACP seeks limited standing to make submissions with respect to those aspects of the Terms of Reference that relate to potential changes in respect of investigations, terrorism prevention, and airline safety.

Disposition

Leave to extend the time to apply for standing is granted, and intervenor status is granted. CACP may, in the first instance, provide written submissions with respect to the aspects of the Terms of Reference as outlined above.

Rules Applicable to All Intervenors

The following rules apply to all intervenors who wish to apply for leave to assume a broader role beyond the filing of written submissions:

Following the filing of their written submissions, intervenors may apply for leave to make a 10 minute opening statement.

Any intervenor wishing to propose a witness to be called by Commission Counsel may make submissions in writing, with reference to Rules of Procedure and Practice 44 and 49, outlining the nature and importance of the anticipated evidence to be given by such witness.

Any intervenor wishing to participate in a manner beyond that envisioned in paragraphs 1 and 2 above, may apply in writing for leave, outlining the nature of the proposed additional participation and attaching submissions as to the unique and valuable contribution to the accomplishment of the mandate of the Commission that would result from such additional participation.

All written submissions and applications are to be submitted in hard copy to Commission Counsel at the address of the Commission, with a copy to the Registrar.

RULING ON STANDING
March 14, 2007
(Aleem Quraishi)

Request by Applicant

Applicant sought full party standing.

Disposition

Party status is granted on the following basis:

The Applicant may participate as provided by the Rules and Terms of Reference with respect to the mandate of the Inquiry. Party status is granted on the understanding that the Applicant will collaborate and align with AICCA as well as with FMCMV/IN.

Rules Applicable to All Intervenors

The following rules apply to all intervenors who wish to apply for leave to assume a broader role beyond the filing of written submissions:

Following the filing of their written submissions, intervenors may apply for leave to make a 10 minute opening statement.

Any intervenor wishing to propose a witness to be called by Commission Counsel may make submissions in writing, with reference to Rules of Procedure and Practice 44 and 49, outlining the nature and importance of the anticipated evidence to be given by such witness.

Any intervenor wishing to participate in a manner beyond that envisioned in paragraphs 1 and 2 above, may apply in writing for leave, outlining the nature of the proposed additional participation and attaching submissions as to the unique and valuable contribution to the accomplishment of the mandate of the Commission that would result from such additional participation.

All written submissions and applications are to be submitted in hard copy to Commission Counsel at the address of the Commission, with a copy to the Registrar.

RULING ON STANDING
May 11, 2007
(Federation of Law Societies of Canada - FLSC)

Request by Applicant

FLSC seeks standing to make submissions with respect to aspects of the mandate of the Inquiry that relate to the legal profession and the administration of the justice system in Canada.

Disposition

Intervenor status is granted. FLSC may, in the first instance, provide written submissions with respect to the aspects of the Terms of Reference as outlined above.

Rules Applicable to All Intervenors

The following rules apply to all intervenors who wish to apply for leave to assume a broader role beyond the filing of written submissions:

Following the filing of their written submissions, intervenors may apply for leave to make a 10 minute opening statement.

Any intervenor wishing to propose a witness to be called by Commission Counsel may make submissions in writing, with reference to Rules of Procedure and Practice 44 and 49, outlining the nature and importance of the anticipated evidence to be given by such witness.

Any intervenor wishing to participate in a manner beyond that envisioned in paragraphs 1 and 2 above, may apply in writing for leave, outlining the nature of the proposed additional participation and attaching submissions as to the unique and valuable contribution to the accomplishment of the mandate of the Commission that would result from such additional participation.

All written submissions and applications are to be submitted in hard copy to Commission Counsel at the address of the Commission, with a copy to the Registrar.

RULING ON STANDING October 29, 2007 GIAN SINGH SANDHU

Order in Council P.C. 2006-293

BEFORE THE COMMISSIONER OF INQUIRY INTO THE INVESTIGATION OF THE BOMBING OF AIR INDIA FLIGHT 182

REASONS

Gain Singh Sandhu has applied for the right to testify on the record at the Inquiry or, in the alternative, to present evidence by way of Affidavit.

Mr. Sandhu states in an Affidavit that certain testimony heard at the hearings of the Inquiry implicates him and his reputation.

A review of the transcript reveals that Mr. Sandhu was referred to in the testimony of James Cunningham and certain remarks were make that might be understood as implicating Mr. Sandhu's reputation.

The subject matter with respect to which the remarks concerning Mr. Sandhu were made is incidental to the mandate of the Commission. Little benefit would be obtained by calling oral evidence on a collateral matter.

On the other hand, Mr. Sandhu should be given an opportunity to respond to the remarks that he believes reflect negatively on his reputation. Accordingly, leave is hereby granted to Mr. Sandhu to submit evidence by way of Affidavit with respect to matters that he believes touch on his reputation as referred to in the evidence of James Cunningham.

John C. Major, Q.C. Commissioner

RULING ON STANDING OCTOBER 29, 2007
APPLICATION FOR BROADER STANDING
WORLD SIKH ORGANIZATION CANADA (WSO)

Order in Council P.C. 2006-293

BEFORE THE COMMISSIONER OF INQUIRY INTO THE INVESTIGATION OF THE BOMBING OF AIR INDIA FLIGHT 182

REASONS

The World Sikh Organization of Canada ("WSO") has applied for broader standing at these hearings. In particular, the WSO seeks a right to cross-examine witnesses on issues related to the reputational interests of the Sikh community and a right to make written and oral submissions on all of the Terms of Reference.

Pursuant to its original application for a standing as an Intervenor, the WSO was given the right to make written submissions with respect to matters touching upon the reputational interests of the Sikh community.

Given its demonstrated expertise and its attendance at many of the hearing dates for this Inquiry, it is appropriate to expand the subject matter of the WSO's Intervenor status to include all of the Terms of Reference on the same terms as currently prevail with respect to other Intervenors.

No Intervenor at these hearings has been granted a right to cross-examine. That right has been reserved for Parties.

It is not appropriate to make an exception in the case of WSO. Like the other Intervenors, the WSO may present written submissions on all matters for which it has now been given the right to intervene. Like the other Intervenors, the WSO may also apply for leave to make oral submissions at the conclusion of the hearing.

John C. Major, Q.C.
Commissioner

WORLD SIKH ORGANIZATION CANADA (WSO)
APPLICATIONS TO CALL CERTAIN WITNESSES

Order in Council P.C. 2006-293

BEFORE THE COMMISSIONER OF INQUIRY INTO THE INVESTIGATION OF THE BOMBING OF AIR INDIA FLIGHT 182

REASONS

The World Sikh Organization of Canada ("WSO") has brought a motion to call three individuals as witnesses at this Inquiry.

The witnesses in question are Gary Bass, Zuhair Kashmeri and David Kilgour.

Pursuant to the *Rules of Practice* of this Inquiry, the first step when an Intervenor proposes that a witness be called is to suggest the name of that witness to Commission Counsel. Commission Counsel have indicated that they intend to call Gary Bass as a witness. Accordingly, insofar as Gary Bass is concerned, this motion is superfluous.

With respect to Zuhair Kashmeri and David Kilgour, the Affidavits submitted on behalf of the WSO indicate that the purpose of calling these witnesses is to deal with the allegation that the Government of India ("GOI") may have been involved in the bombing of Air India Flight 182 and that this allegation was not investigated adequately in the aftermath of the bombing.
\
A review of the Terms of Reference of this Commission of Inquiry reveals that the investigation of the bombing of Air India Flight 182 is intended to serve as a backdrop and reference point for issues as to the degree of co-operation demonstrated between the departments and agencies of the Government of Canada, including the RCMP and CSIS. The investigation is also intended to present a reference point for the issue of transforming security intelligence into evidence admissible in a criminal trial.

None of the Terms of Reference calls for an inquiry into the issue of who was responsible for the bombing of Flight 182 nor of the role, if any, of the GOI, nor of the thoroughness of the investigation of any such role by the RCMP and/or CSIS. This contrasts with the mandate of the 1991-92 SIRC Review.

Since the subject matter of the WSO's request is not to be found in our Terms of Reference, the motions to call oral evidence on that subject through Messrs. Kashmiri and Kilgour are hereby dismissed.

John C. Major, Q.C.
Commissioner

The Canadian Bar Association (CBA)
June 13, 2007

RULING ON OPENING STATEMENT

Request by Applicant

The Canadian Bar Association sought leave to make an opening statement during Stage 2 of the Inquiry proceedings so that the CBA can address the issues that are of concern to the CBA and are within the Commissioner's mandate.

Disposition

The Canadian Bar Association may make an opening statement for up to 30 minutes to highlight the key points outlined in their written submission. The written submission can be filed as Inquiry evidence at that time. The CBA is requested to coordinate with Commission counsel to arrange an appropriate time for making the opening statement.

It is also envisaged that Commission counsel may also find an occasion as appropriate to afford the CBA another opportunity to present oral testimony through participation in a panel. Commission counsel will contact the CBA at a later date if this opportunity arises.

Air India Victims Families Association (AIVFA)
January 3, 2007

REASONS FOR DECISION WITH RESPECT TO THE AIVFA'S REQUEST FOR DIRECTIONS REGARDING ACCESS TO UNREDACTED DOCUMENTS AND *IN CAMERA* AN EX PARTE HEARINGS

INTRODUCTION

1. This motion for direction is dismissed. The families in this Inquiry have been promised full participation in the Air India Inquiry in accordance with Terms of Reference. The failure of this application requires a full explanation as to why the limit on their counsel attending *in camera* hearings or viewing redacted (edited) documents that could have been injurious to international relations, national defence or national security (hereinafter collectively referred to as "national security") is necessary and does not hamper the families participation.

2. Counsel for the families correctly acknowledge that if they were able to attend the *in camera* hearings, of which there have not been any as of yet, and or view security related documents they are and would be prohibited by law from disclosing, however innocuous, any aspects of those proceedings or documents to their clients who are members or relations of the families of the victims of the Air India explosion. That raises the question of what possible value such attendance or viewing documents would be to the families.

3. As a corollary to that restriction there is an obligation on this Commission to ensure to the extent possible that all hearings and document production be public. The reasons for hearings and production *in camera* camera for reasons of national security, which encompasses all Canadians, must be clearly demonstrated to the commission by the Government of Canada ("G.O.C.") when such procedure is sought.

4. While counsel are not entitled to attend *in camera* hearings, they are entitled to make submissions and call relevant evidence if any, to show that the particular request by the G.O.C. for an *in camera* hearing should not be ordered. The only basis for having the *in camera* hearings will be if the G.O.C. has demonstrated that the matter involved could in the opinion of the Commissioner, be injurious to national security.

5. The foregoing summary needs elaboration. The elaboration is intended to explain that any fear by the families of being excluded, misinformed or not being able to fully participate within the terms of reference is misplaced. The absence of their counsel from *in camera* hearings on national security will not affect their full participation.

THE POSITION OF THE PARTIES

6. AIVFA submits that their counsel who have top secret clearance granted by the Government of Canada be admitted to *in camera* hearings and be granted access to unredacted documents. They submit there should be no national security concerns in allowing them to participate in *in camera* hearings and to see unredacted documents. Their counsel further submits that for them to have this access would ensure that AIVFA will be engaged, through its counsel, as a full contributor to the Commission's work while increasing the confidence and trust of family members in the Inquiry itself. AIVFA points specifically to the goal alluded to at the end of Stage 1 of the Inquiry, namely "to ensure that when parties leave this hearing that they feel they have had a full opportunity to explore the cause [of the failure to prevent the bombing] and be satisfied they know what happened to the extent that is possible." AIVFA submits that the access it seeks for its counsel is a means to achieve this goal and that nothing in the Inquiry's Terms of Reference prevents me from granting the direction or order being sought.

7. The Government of Canada opposes the motion. In support of its position, it cites the Terms of Reference of the Inquiry and the procedures set out in Section 38 of the Canada Evidence Act for dealing with top secret matters as well as the way national security is treated in other legal proceedings. G.O.C. submits that the Terms of Reference and the procedure set out in Section 38 preclude counsel for AIVFA, although holding top security clearance, being granted the access sought.

DISPOSITION

8. The explicit provisions of the Terms of Reference of this Inquiry and the procedural provisions outlined in Section 38 of the Canada Evidence Act support G.O.C. application preclude me from granting AIVFA counsel the access requested. From a functional point of view, even if I did have jurisdiction to grant access, it is difficult to see how such access could improve the knowledge or understanding of the families with respect to the subject matter of the Inquiry. Even if such access were possible, it would serve no practical benefit for the families themselves as penal sanctions prevent any disclosure to anybody including their clients of anything seen or heard at the *in camera* hearings or in unredacted documents. G.O.C. also submits that if the issue is seen as one of fairness, there are other guarantees of fairness in the Inquiry process that make the access sought unnecessary.

9. I agree that the concern advanced by the families demonstrates the necessity of holding as much of this Inquiry as possible in public but, that fact does not give me jurisdiction to allow the motion for attendance applied for.

IN CAMERA HEARINGS

10. Unlike a court of inherent jurisdiction, a Commission of Inquiry only has the powers granted to it by statute or by its Terms of Reference. The Commission's Powers and Duties respecting the matters raised by AIVFA are found at paragraphs d, f, m, n and o of the Terms of Reference:

that the Commissioner be authorized to adopt any procedures and methods that he may consider expedient for the proper conduct of the Inquiry, and to sit at any times and in any places in or outside Canada that he may decide

that the Commissioner be authorized to grant to the families of the victims of the Air India Flight 182 bombing an opportunity for appropriate participation in the Inquiry

the Commissioner, in conducting the Inquiry, to take all steps necessary to prevent disclosure of information which, if it were disclosed, could, in the opinion of the Commissioner, be injurious to international relations, national defence or national security and to conduct the proceedings in accordance with the following procedures, namely,

(i) on the request of the Attorney General of Canada, the Commissioner shall receive information *in camera* and in the absence of any party and their counsel if, in the opinion of the Commissioner, the disclosure of that information could be injurious to international relations, national defence or national security

that nothing in that Commission shall be construed as limiting the application of the provisions of the *Canada Evidence Act*

the Commissioner to follow established security procedures, including the requirements of the *Government Security Policy,* with respect to persons engaged pursuant to section 11 of the *Inquiries Act* and the handling of information at all stages of the Inquiry.

11. At present AIVFA's request with respect to access to *in camera* proceedings is premature since there has not been any request by the Attorney General of Canada as set out in paragraph m(i) of the Terms of Reference, nor have I made any ruling to date that any session be *in camera*. However, undoubtedly such a request will be made and that it is necessary to determine the principles at this point, that will govern the conduct of *in camera* hearings. This provides procedural clarity and it is hoped will avoid unnecessary delay if such a request is made.

12. It should be noted that a mere request by the Attorney General of Canada is not sufficient to obtain an order that some particular matter be heard *in camera*. Pursuant to paragraph m(i) of the Terms of Reference, the Attorney General must satisfy me that disclosure of the information in question could be injurious to international relations, national defence or national security before I can

order that the information be dealt with through *in camera* hearings. G.O.C. concedes that the parties in this Inquiry, including AIVFA through its counsel, have a right to make submissions in response to any such request and to oppose any specific request for an *in camera* hearing.

13. Paragraph m(i) of the Terms of Reference is clear that if I am satisfied by the Attorney General that disclosure of such information could be injurious to international relations, national defence or national security, I have no jurisdiction other than I "shall" receive the information "*in camera* and in the absence of any party and their counsel."

14. Paragraph d. of the Terms of Reference, which authorizes me to adopt any procedures and methods that I may consider expedient for the proper conduct of the Inquiry does not allow me to modify or ignore the clear instructions set out in paragraph m(i). I disagree with the proposed reading by AIVFA of paragraph m(i) which would, for purposes of the present motion, read the test to be whether "disclosure of that information and could be injurious…" as meaning that I should assess whether "disclosure *to counsel with top secret clearance* of that information could be injurious …". I do not agree with this innovative argument as it is inconsistent with the express requirement that information, the disclosure of which could be harmful, must be received *in camera* "and the absence of any party *and their counsel*." Wording to prevent this result could easily have been used had that been the G.O.C. intent.

ACCESS TO UNREDACTED DOCUMENTS

15. Paragraph n of the Terms of Reference provides that nothing in the Terms of Reference establishing the Commission is to be construed as limiting the application of the provisions of the *Canada Evidence Act*.

16. Pursuant to Section 38.11(2) of that *Act*, the Attorney General is entitled to make *ex parte* representations (i.e. representations outside of the presence of any party or its counsel) concerning the redaction of sensitive or potentially injurious information. I am not bound to accept the submissions of the Attorney General and Commission counsel may argue either in support of or in opposition to these submissions, but there is no doubt that the redaction process is not one in which counsel for the parties, with or without security clearance, may participate. I agree with the Attorney General's submission, that sensitive or potentially injurious information must be redacted from documents prior to their use in public hearings and that there is nothing that authorizes me to grant counsel for AIVFA access to unredacted versions of such documents.

FUNCTIONAL CONSIDERATIONS

17. A consideration of the functional implications of the directions being requested by AIVFA reinforces the conclusions that I have reached.

18. Counsel for G.O.C. submits the case law with respect to national security issues makes it clear that the potentially injurious consequences of disclosure have lead courts to take a very cautious approach. See *Secretary of State for the Home Department v. Rehman,* [2001] 3 W.L.R. 877. The principle stated there was accepted by the Supreme Court of Canada in *Suresh v. Canada (Minister of Citizenship and Immigration),* [2002] 1 S.C.R. 3 at para. 33:

"It is not only that the executive has access to special information and expertise in these matters [of national security]. It is also that such decisions, with serious potential results for the community, require a legitimacy which can be conferred only be entrusting them to persons responsible to the community through the democratic process."

19. The principle that has been adopted by the Government of Canada in dealing with disclosure of information potentially injurious to national security or to the national interest, is to restrict disclosure on the basis of "need to know". This principle has been approved by the Federal Court of Appeal in connection with the "informer privilege" in *Canada (R.C.M.P. Public Complaints Commission) v. Canada (Attorney General),* 2005 FCA 213*. There, disclosure was sought by the RCMP Complaints Commissioner in order to "ensure the highest possible standard of justice." Lètourneau J.A. responded that "as laudable as this goal may be, it cannot justify granting access to persons who are not persons who need to know such information for law enforcement purposes." (paras 43-48)

20. This same "need to know" principle should be applied with respect to *in camera* hearings and access to unredacted documents. In the present circumstances, it cannot be said that in their role as counsel, counsel for AIVFA "need to know" the information to which access is being sought. As AIVFA acknowledges, counsel would not be able to disclose any information learned in the course of the *in camera* hearings nor could they disclose the redacted portions of documents to their clients. AIVFA explicitly acknowledges that counsel would be required to give an undertaking not to make such disclosure. In those circumstances, it is impossible to see how access to *in camera* hearings or unredacted documents would add to the families' "opportunity to explore the cause" or allow them "to be satisfied that they know what happened." Counsel themselves might believe that they had more information about what happened, but they could not communicate that information to their clients. This would not justify treating granting of access as capable of outweighing the Government's interest in restricting disclosure, and that would be the case even if the Terms of Reference allowed me to do such balancing, which, they do not. In fact, even if they were allowed to attend *in camera* sessions, counsel for AIVFA could only subsequently make arguments and submissions as if they had not attended them.

21. It is important that the public interest (which includes the interest of the families) with respect to a full exploration of all the facts is not left unguarded. At the restricted *in camera* hearing and/or the redaction of document it is the responsibility of the Commission and the role of Commission counsel to protect that public interest. As noted by Mr. Justice Dennis O'Connor, Commissioner at

the Arar Inquiry, in his non-judicial article, "The Role of Commission Counsel in a Public Inquiry":

"… commission counsel's role is not to advance any particular point of view, but rather to investigate and lead evidence in a thorough, but completely impartial and balanced manner. In this way, the commissioner will have the benefit of hearing all the relevant evidence unvarnished by the prospective of someone with an interest in a particular outcome." (2003), 22 Advocates Soc. J. No. 1, at para. 12.

22. As also noted by Justice O'Connor, where a public inquiry does hear evidence *in camera*, the role of Commission counsel in representing the public interest allows Commission counsel to depart somewhat from his or her normal role and to engage in pointed cross-examination where necessary, so as to ensure that evidence heard *in camera* is thoroughly tested -- a procedure intended to be followed by this Commission.

CONCLUSION

23. There is no doubt, as submitted by AIVFA, that there is a valid interest in the fullest possible airing of all information relevant to the subject matter of the Inquiry. For that reason, to the extent that it is possible, hearings should be public and the information disclosed publicly. That is the principle set out in rule 22 of our Rules of Practice and Procedure. The operative concept, however, is the phrase "to the extent that that is possible", words that I also used in the passage cited by AIVFA in describing the educational goal of the Inquiry.

24. By the Terms of Reference of this Inquiry, I have no jurisdiction to grant access to counsel for AIVFA to any *in camera* hearings that may be held nor to unredacted versions of documents that have been redacted for national security reasons. Functional considerations, including the deference due to government with respect to matters touching on national security and the appropriateness of the "need to know" principle, lead in the present case, to the same result. For all the above as previously stated this application for direction is dismissed.

ANNEX B: PARTIES AND INTERVENORS

PARTIES

Attorney General of Canada represented by:
Barney Brucker, Department of Justice Canada

Air India represented by:
Soma Ray-Ellis, Patterson, MacDougall LLP

Air India Cabin Crew Association (AICCA) represented by:
Richard P. Quance and Darren James Smith, Himelfarb Proszanski LLP

Air India Victims Families Association (AIVFA) represented by:
Norman Boxall, Bayne Sellar Boxall
Jacques J.M. Shore and Chris Schafer, Gowling Lafleur Henderson LLP

Family members of the crew member victims of Air India Flight 182 and Indian nationals represented by:
Richard P. Quance and Darren James Smith, Himelfarb Proszanski LLP

Sanjay Lazar represented by:
Richard P. Quance and Darren James Smith, Himelfarb Proszanski LLP

Lata Pada represented by:
Raj Anand and April Brosseau, WeirFoulds LLP

Aleen Quraishi represented by:
Richard P. Quance and Darren James Smith, Himelfarb Proszanski LLP

Niraj Sinha

INTERVENORS

B'nai Brith Canada represented by:
Adam Goodman, Heenan Blaikie LLP

Canadian Association of Chiefs of Police (CACP) represented by:
Vincent Westwick

The Canadian Bar Association (CBA) represented by:
Lorne A. Waldman, Waldman & Associates
Greg Del Bigio

Canadian Civil Liberties Association (CCLA) represented by:
A. Alan Borovoy

Canadian Coalition Against Terror (C-CAT) represented by:
Aaron Blumenfeld and Amy Westland, Borden Ladner Gervais LLP

Canadian Coalition for Democracies (CCD) represented by:
David B. Harris

Canadian Council on American Islamic Relations (CAIR-CAN) and **Canadian Muslim Civil Liberties Association (CMCLA)** represented by:
Faisal Kutty and Akbar Sayed Mohamed, Kutty, Syed & Mohamed

Canadian Jewish Congress (CJC) represented by:
Lawrence Thacker, Lenczner Slaght

Canadian Resource Centre for Victims of Crime (CRCVC)

Criminal Lawyers' Association (CLA) represented by:
Paul Burstein, Burstein, Unger

Federation of Law Societies of Canada (FLSC)

Ripudaman Singh Malik represented by:
Murray L. Smith, Smith Barristers

World Sikh Organization of Canada (WSO) represented by:
Palbinder Shergill, Shergill and Company

ANNEX C: COMMISSION OF INQUIRY STAFF AND CONSULTANTS

Commissioner's Office
Major, Hon. John C. - Commissioner
Kenny, Barbara - Executive Assistant to the Commissioner (Calgary)
Archdeacon, Maurice - Special Advisor to the Commissioner

Executive
Brook, Dennis - Director - Operations
Cooke, Lynne - Director - Finance

Administrative Staff
Ariano, Wanda
Brisson, Richard
Cécire, Angelo
Dickerson, Ken
Duquette, Julie
Fitzsimmons, Donna
Guérin, Kim
Godbout, Gail
Hooper, Anne
Irani, Lina
Karmali, Nadia
Monette, Pierre
Mutton, Mary
Osborne, Anita
Rock, Stephanie
Surprenant, Roland
Thomas, Roger

Report Production
Editing:
Gussman, Tom
Sadinsky, Ian
Oscapella, Eugene
S&D Jung
Enman, Charles
Fowler, Rod
Duquette, Julie
Translation:
Translation Bureau (PWGSC)

Design & Production
Fitzsimmons, Donna
Formatting
Burritt, Denise
Guérin, Kim

Legal
Freiman, Mark – Commission Lead Counsel
Dorval, Michel – Co-Counsel

Bilodeau, Roger – Senior Counsel
Gover, Brian – Senior Counsel
Kapoor, Anil – Senior Counsel

Barragan, Francis
Blum, Nadine
Boucher, Alexandre
Bowes, Tanya
Carle, Frédéric
Coutlée, Geneviève
Fairchild, Robert
Mall, Adela
Marshman, Nigel
Perron, Jean-Paul
Rachamalla, Teja
Saito, Yolanda
Sévéno, Louis
Victor, Marisa
Viswanathan, Hari
Vancouver:
Gudmundseth, Stein
Michelson, Howard
Dosanjh, Arpal
Gartner, Janet

Research
Archambault, Dr. Peter
Roach, Prof. Kent

Hearings
International Reporting (Court Reporters)
PWGSC Translation Bureau (Interpretation Services)

Website
Baytek Systems

Other
Brisson, Gilles – Registrar
Tansey, Michael – Media Advisor

Special Thanks
Special Thanks to all those at the Privy Council and PWGSC who helped the Commission in so many ways; with special mention to Mark Amodeo of PCO IT and Denise Larocque of PCO Corporate Services.

Last Name	First Name	Organization/ Family Member
Abda	Laxmansinh Jayantkumar	Family member
Abid	Jainul ("Joe")	Formerly with Air India
Alemán	Moses	Civil aviation security expert
Alexander	Rob	Family member
Anand	Anita	University of Toronto Faculty of Law
Atkey	Ronald ("Ron")	Former Chairman of the Security Intelligence Review Committee
Aubin	Michel	Royal Canadian Mounted Police
Baggaley	Carman	Office of the Privacy Commissioner of Canada
Bailey	Smita	Family member
Bains	Rajvinder (Singh)	Punjabi Human Rights Organization
Barrette	Jean	Transport Canada
Bartleman	James K.	Formerly with Foreign Affairs and International Trade Canada
Basnicki	Maureen	Canadian family member of 9/11 victim
Bass	Gary	Royal Canadian Mounted Police
Beauchesne	Eric	Family member
Beaulieu	Marc	Quebec Ministry of Public Security

Last Name	First Name	Organization/ Family Member
Bedi	Parkash	Family member
Bertram	Jim	Greater Toronto Airport Authority
Best	Douglas	Royal Canadian Mounted Police
Bettman	Michael	Correctional Service of Canada
Bhinder	Amarjit	Family member
Blachford	Bart	Royal Canadian Mounted Police
Blair	William	Toronto Police Service
Bloodworth	Margaret	Privy Council Office
Boisvert	Anne-Marie	Faculty of Law, University of Montreal
Bonneau	Régis	Royal Canadian Mounted Police
Bourgault	Jacques	Université du Québec à Montréal
Brandt	Brion	Transport Canada
Brodeur	Jean-Paul	Centre international de criminologie comparée, Université de Montréal
Bromley	Blake	Benefic Group
Brown	Daniel	Crew, Laurentian Forest (Recovery)
Browning	Greg	Royal Canadian Mounted Police

Last Name	First Name	Organization/ Family Member
Burgoyne	Robert ("Bob")	Formerly with the Canadian Security Intelligence Service
Burns	Robert	CanPro Pacific Services Inc.
Carignan	Serge	Formerly with the Quebec Provincial Police
Carlson	Gary	Royal Canadian Mounted Police
Carter	Terrance	Carters Professional Corporation (Carters)
Cartwright	Nick	Transport Canada
Castonguay	Monique	Family member
Chabot	Steven	Sûreté du Québec
Chesney	Robert	Wake Forest University
Chopra	Rajesh	Air India
Clarke	Gary	Formerly with the Royal Canadian Mounted Police
Code	Michael	University of Toronto Faculty of Law
Comeau	Michael	New Brunswick Department of Justice and Consumer Affairs
Conrad	Stephen	Transport Canada
Crook	Rick	Formerly with the Vancouver Police Department
Cunningham	Jim	Royal Canadian Mounted Police

Last Name	First Name	Organization/ Family Member
Cyr	Pierre	Canadian Air Transport Security Authority
Dandurand	Yvon	University College of the Fraser Valley
De March	Terry	Canada Revenue Agency
Desjardins	Robert	Foreign Affairs and International Trade Canada
Dewhirst	David	Formerly with Foreign Affairs and International Trade Canada
Dibble	Kenneth	Charity Commission for England and Wales
Dicks	Ron	Formerly with the Royal Canadian Mounted Police
DiFrancesco	Janet	Financial Transactions and Reports Analysis Centre of Canada
Dolhai	George	Public Prosecution Service of Canada
Doran	Tom	Garda (Ireland)
Dosanjh	The Honourable Ujjal	MP and prominent member of BC Sikh community
Douglas	Wayne	Formerly with the Royal Canadian Mounted Police
Doyon	Louise	Canadian Security Intelligence Service
Duff	David	University of Toronto Faculty of Law
Duguay	Yves	Air Canada

Last Name	First Name	Organization/ Family Member
Elliott	William	Royal Canadian Mounted Police
Ellis	Andrew	Canadian Security Intelligence Service
Eshleman	Neil	Formerly with the Canadian Security Intelligence Service
Frisby	Geoff	Formerly with the Royal Canadian Mounted Police
Galt	Jim	Canadian Security Intelligence Service
Gartshore	Glen	Formerly with the Canadian Security Intelligence Service
Gaul	Geoff	British Columbia Ministry of the Attorney General
Gaur	Saroj	Family member
George	Tyson	Canada Border Services Agency
Giasson	Daniel	Integrated Threat Assessment Center, Canadian Security Intelligence Service
Gibbs	Colin	Crown Prosecution Service (UK)
Gillies	John A.	Canadian Security Intelligence Service
Gogia	Ram	Family member
Gopalan	Ramachandran	Family member
Goral	Terry	Formerly with the Royal Canadian Mounted Police
Graham	Georgina	International Air Transport Association

Last Name	First Name	Organization/ Family Member
Grenier	Justice Bernard	Comité du Barreau du Québec
Grierson	Mervin	Formerly with the Canadian Security Intelligence Service
Gupta	Anita	Family member
Gupta	Bal	Family member
Gupta	Shailendra	Family member
Gupta	Susheel	Family member
Hall	Craig	Air Line Pilots Association International
Hanse	Anil	Family member
Hayer	David ("Dave")	Son of Tara Singh Hayer, slain Sikh journalist in BC
Hayes	Thomas	Garda (Ireland)
Heatherington	Scott	Foreign Affairs and International Trade Canada
Heed	Chern	Expert consultant - Airports
Hennessy	Michael	Department of History, Royal Military College
Henry	John	Formerly with the Canadian Security Intelligence Service
Henschel	Lyman	Formerly with the Royal Canadian Mounted Police
Hickman	Lloyd	Formerly with the Royal Canadian Mounted Police

Last Name	First Name	Organization/ Family Member
Hoffman	Bruce	Georgetown University
Hooper	Jack	Formerly with the Canadian Security Intelligence Service
Hovbrender	Axel	Vancouver Police Department
Inkster	Norman	Formerly with Royal Canadian Mounted Police
Jagoe	Jamie	Royal Canadian Mounted Police
Jardine	James	Former Crown Counsel, Department of the Attorney General, British Columbia
Jarrett	Lynne (formerly Lynne McAdams)	Formerly with the Canadian Security Intelligence Service
Jensen	Henry	Formerly with the Royal Canadian Mounted Police
Jobin	Pierre-Côme	Quebec Ministry of Public Security
Jodoin	Jacques	Formerly with the Canadian Security Intelligence Service
Jones	Fred	Canadian Airports Council
Judd	Jim	Canadian Security Intelligence Service
Kachroo	Meera	Family member
Kachru	Vijay	Family member

Last Name	First Name	Organization/ Family Member
Kalsi	Rattan (Singh)	Family member
Kaushik	Neelam	Family member
Kelly	Phillip	Garda (Ireland)
Kennedy	Paul	Commission for Public Complaints against the RCMP
Kenny	The Honourable Colin	Chair, The Standing Senate Committee on National Security and Defence
Khandelwal	Deepak	Family member
Khandelwal	Ramji	Family member
Kirwan	Peter	Garda (Ireland)
Klein	Maurice	Canada Revenue Agency
Kobzey	Ray	Formerly with the Canadian Security Intelligence Service
Kosseim	Patricia	Office of the Privacy Commissioner of Canada
Krindle	Ruth	Formerly with the Manitoba Court of Queen's Bench
Kumar	T. N.	Air India
Labbé	Jean	Air Line Pilots Association, International

Last Name	First Name	Organization/ Family Member
LaCompte	Pierre	Canadian Security Intelligence Service
Lafleur	Diane	Department of Finance Canada
Lalonde	Daniel	Formerly with Burns Security
Lalonde	Mark	CanPro Pacific Services Inc.
Lane	Duncan	Canadian Security Intelligence Service
Lapointe	Pierre	Steering Committee on Justice Efficiencies and Access to the Criminal Justice System (Department of Justice - Canada)
Laurie	William Dean ("Willie")	Formerly with the Canadian Security Intelligence Service
Lazar	Sanjay	Family member
Leiss	Dr. William	University of Ottawa
Lyon	David	Queen's University
MacBrayne	John	Metropolitan Police Service (London, UK)
MacDonald	J.B. ("Joe")	Formerly with the Royal Canadian Mounted Police
MacDonald	Michael Anne	Formerly with the Ministry of the Attorney General, Ontario
MacDonell	Laurie	Royal Canadian Mounted Police

Last Name	First Name	Organization/ Family Member
MacFarlane	Bruce	University of Manitoba
MacNeil	Alphonse	Royal Canadian Mounted Police
Madon	Natasha	Family member
Madon	Perviz	Family member
Malizia	James	Royal Canadian Mounted Police
Mamak	Kalwant	Family member
Marriott	Jim	Transport Canada
Martinez-Hayer	Isabelle	Daughter-in-law of Tara Singh Hayer, slain Sikh journalist in BC
Mattson	Dale	Formerly with Transport Canada
Mayer	Dan	Royal Canadian Mounted Police
McDonell	Mike	Royal Canadian Mounted Police
McLean	Don	Formerly with the Vancouver Police Department
Molgat	Daniel	Formerly with Foreign Affairs and International Trade Canada
Morden	Reid	Formerly with the Canadian Security Intelligence Service

Last Name	First Name	Organization/ Family Member
Morrill	Keith	Department of Foreign Affairs and International Trade
Morris	Pat	Ontario Provincial Police
Muir	R.E.	Formerly with the Royal Canadian Mounted Police
Murphy	Seanie	Captain Royal National Lifeboat Institution (Recovery)
Murray	Dave	Canadian Security Intelligence Service
Nash	William	Transport Canada
Newham	Paul	National Terrorist Financial Investigation Unit (UK)
Normand	Gérard	Formerly with the National Security Group
Norris	John	Ruby & Edwardh, LLP
O'Brian	Geoffrey	Canadian Security Intelligence Service
Pada	Lata	Family member
Parsons	Ches	Royal Canadian Mounted Police
Passas	Nikos	Northeastern University College of Criminal Justice
Passmore	Neil	Canadian Security Intelligence Service, (presently seconded to the Royal Canadian Mounted Police)
Paul	Donna Ramah	Family member

Last Name	First Name	Organization/ Family Member
Paulson	Bob	Royal Canadian Mounted Police
Person 1		Source who warned of plot against Air India
Piché	Catherine	Quebec Ministry of Public Security
Pichette	Pierre-Paul	Service de police de la Ville de Montréal
Pinos	Graham	Formerly with the Department of Justice Canada
Portelance	Luc	Canadian Security Intelligence Service
Potter	Mark	Financial Transactions and Reports Analysis Centre of Canada
Quartermain	David	Canada Border Services Agency
Quiggin	Thomas	Nanyang Technological University
Quraishi	Aleem	Family member
Radhakrishna	Haranhalli	Family member
Rae	The Honourable Bob	Author of *Lesssons to be Learned*
Rai	Satrajpal	Family member
Ramakesavan	Ramu	Family member
Rana	Shipra	Family member
Razack	Sherene	University of Toronto

Last Name	First Name	Organization/ Family Member
Reynolds	Rick	Royal Canadian Mounted Police
Roach	Kent	University of Toronto Faculty of Law
Roth	Michael ("Mike")	Formerly with the Royal Canadian Mounted Police
Rudner	Martin	Carleton University
Sabharwal	Promode	Family member
Sahota	Manjit (Singh)	Sikh community activist (Toronto)
Saklikar	Renee	Family member
Sandhu	Gian Singh	Former president of World Sikh Organization of Canada
Sangollo	Pierre	Correctional Service of Canada
Sankurathri	Chandra	Family member
Schmidt	John	Integrated Threat Assessment Center, Canadian Security Intelligence Service
Schwartz	Lorne	Royal Canadian Mounted Police
Scotton	Lindsay	Office of the Privacy Commissioner of Canada
Scowen	Chris	Formerly with the Canadian Security Intelligence Service
Sharma	Krishna	Family member

Last Name	First Name	Organization/ Family Member
Sharma	Mahesh Chandra	Family member
Sharma	Usha	Family member
Sharma	Veena	Family member
Sheahan	William ("Bill")	Formerly with the Communications Security Establishment
Sheehan	Terry	Formerly with Foreign Affairs and International Trade Canada
Sidel	Mark	University of Iowa College of Law
Simmonds	Robert	Formerly with the Royal Canadian Mounted Police
Simpson	Brian	Formerly with Air Canada
Singh	Sarabjit	Punjabi Human Rights Organization
Smith	Gordon	Formerly with Foreign Affairs and International Trade Canada
Solvason	Robert	Formerly with the Royal Canadian Mounted Police
Souccar	Raf	Royal Canadian Mounted Police
Stagg	Mark	Crew, Laurentian Forest (Recovery)
Steinberg	Ralph	The Chief Justice's Advisory Committee on Criminal Trials in the Superior Court of Justice (Ontario)

Last Name	First Name	Organization/ Family Member
St. John	Peter	University of Manitoba
Stevenson	John	Formerly with the Canadian Security Intelligence Service
Stewart	Gavin	Formerly with Foreign Affairs and International Trade Canada
Stoddart	Jennifer	Privacy Commissioner of Canada
Stubbings	Bob	Formerly with the Royal Canadian Mounted Police
Sweeney	Steve	Vancouver Police Department
Sweeney	Warren	Formerly with the Royal Canadian Mounted Police
Sweet	Kathleen	University of Connecticut
Tait	Mark	Royal Air Force diver (Recovery)
Tario	Brian	Deloitte
Taylor	Kim	Integrated Threat Assessment Center, Canadian Security Intelligence Service
Thampi	Jayashree	Family member
Thompson	Brent	British Columbia Ministry of the Attorney General
Townshend	Ron	British Columbia Registry Services

Last Name	First Name	Organization/ Family Member
Tremblay	Larry	Royal Canadian Mounted Police (presently seconded to Canadian Security Intelligence Service)
Trudel	Reg	Royal Canadian Mounted Police
Turlapati	Padmini	Family member
Turner	Bill	Canadian Security Intelligence Service
Turner	Trevor	Royal Canadian Mounted Police
Upton	Russell	Formerly with the Canadian Security Intelligence Service
Vaidyanathan	Chandra	Family member
Vaney	Herbert	Formerly with Air India
Venketeswaran	Ann	Family member
Venketeswaran	Esther	Family member
Vinette	Denis	Canada Border Services Agency
Wall	Robert	Formerly with the Royal Canadian Mounted Police
Wallis	Rodney	International civil aviation security consultant
Walsh	Donna	Canada Revenue Agency

Last Name	First Name	Organization/ Family Member
Warden	William	Formerly with Foreign Affairs and International Trade Canada
Wark	Wesley	Munk Centre for International Studies, University of Toronto
Warren	James ("Jim")	Formerly with the Canadian Security Intelligence Service
Whitaker	Reg	York University
Zaccardelli	Giuliano	Formerly with the Royal Canadian Mounted Police
Zelmer	Daryl	Formerly with the Canadian Security Intelligence Service