Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1997-98

This part of the audit report presents the results of major research and analysis carried out by the Committee in the course of the year. The special inquiries are in addition to, and are intended to complement and reinforce, the other forms of audit research the Committee undertakes.

The Committee's selection of topics to be the subject of in-depth inquiry is influenced by a number of factors including *inter alia*, shifts in the nature of the international threat environment, changes in technology, the need to monitor the impact of or follow up on past Committee recommendations, significant alterations in Government policy which the Committee believes could have implications for Service activities, changes in organizational structure or operational emphasis within the Service itself, and the interests of individual Committee Members.

This year, the subjects of the Committee's special interest are the following: CSIS investigations into urban political violence; the Meshal incident in Amman, Jordan; the Service's role in immigration screening; matters surrounding a foreign conflict and several domestic threats; intra-governmental cooperation in matters of economic security; policies and procedures for exchanging information with law enforcement agencies and other government departments; the Service's liaison program with foreign intelligence agencies; and, the first phase of our review of CSIS cooperation with the Royal Canadian Mounted Police.

In addition, the Committee reports on four other studies that were smaller in scope — the first concerns the Service's policies regarding "sensitive" institutions, the second looks into the handling of a particular human source operation, the third reviews the remedial measures arising from a breach of security which occurred within the Service, and the fourth looks at a counter intelligence case of historical interest.

Urban Political Violence

Report #94

In 1997 we examined four CSIS investigations of Canadian persons and organizations conducted under section 12 and paragraph 2(c) of the *CSIS Act* — that part of the Service's mandate which directs it to investigate threats of "serious violence" for the purpose of achieving a political objective, more commonly known as the "counter terrorism" clause. What drew the Committee's attention to this particular set of cases was in part a need to reassure ourselves that CSIS was not conducting counter subversion investigations under its counter terrorism mandate. Investigations and their accompanying targeting authorities conducted under section 2(d) of the *Act* — the "counter subversion" clause — require the personal authorization of the Minister,[1] a step not normally required for other kinds of investigation.

As with most of the Committee's reviews, our evaluation also considered whether the Service had reasonable grounds to suspect a threat, whether the level of the investigation was proportionate to the seriousness and imminence of the threat, and whether the information collected was strictly necessary. In the course of our review, SIRC researchers had access to all CSIS reports and files generated during the investigations.

The Committee's Findings

The first two cases dealt with a series of violent incidents which occurred in the mid-1990's. We concluded that the Service did have reasonable grounds to suspect a threat to national security and that only information strictly necessary to provide advice to the government was collected.

However, the Committee also observed difficulties in the relationship between the Service and the police agency leading the criminal investigation that was simultaneously underway against the same targets. The friction between the two agencies centered on the disclosure requirements imposed by the Courts since the R. v Stinchcombe decision. [See inset page 31]

Under the police force's interpretation of the decision, any information it possessed — verbal or written, formal or informal, and regardless of source — was subject to disclosure to the Courts. The Service, in order to protect the integrity and security of its investigations and methods responded to this position by carefully filtering its exchanges with the police force in question. While the Committee is satisfied that the impact of the disagreement was local and temporary, the Committee will continue to monitor the repercussions, if any, of the Stinchcombe decision for CSIS operations and inter-agency relations, especially in the counter terrorism area.

The third case we examined was an issue-based investigation that spanned the country, but focused primarily on Toronto and Vancouver. Of the over 200 field reports the investigation generated, two were not strictly necessary in our view. In the first, the information collected did not deal with violent activity of any sort. The Service agreed with our observation and subsequently deleted the report from its data base. The second report we questioned dealt with the visit to Canada of a representative of a political party of a foreign country. While the Committee did not originally accept the rationale for CSIS involvement in this matter, information we have since received from the Service leads us to conclude that a potential threat to national security was indeed present.

In the fourth investigation reviewed, we identified no problems.

Counter Terrorism or Counter Subversion?

With respect to whether the investigations were conducted under the appropriate section of the *Act*, the Committee is satisfied that the four investigations were properly authorized. The selection of targets, as well as all investigative activities and reporting, were based on the potential for violence to achieve a political objective, and not the nature of the political opinions themselves.

The Committee will continue to monitor the repercussions, if any, of the Stinchcombe decision for CSIS operations and inter-agency relations

In addition, the investigative techniques used were proportionate to the threat.

Operational Cooperation and the Meshal Incident

The Committee found no evidence that CSIS was involved in any manner with the Meshal-Amman incident

The media reported that on 25 September 1997, two agents of the Israeli intelligence service Mossad carrying Canadian passports attempted to assassinate Khaled Meshal, an official of the Palestinian organization Hamas,[2] in Amman, Jordan. The attempt failed, and Jordanian authorities seized the agents and the passports. The incident, and the use of Canadian passports by Israel's intelligence service, raised a number of questions, some of which were prominent in various media at the time, about CSIS cooperation with foreign agencies.

The Review Committee devoted considerable effort to examining the events surrounding this incident not least because of the serious nature of the allegations — that CSIS may have been a party to an assassination attempt in a foreign country.

Methodology of SIRC's Review

In order to understand how and whether CSIS was involved in the Meshal incident, we examined all Service files with a possible connection to the matter, as well as those that pertained to Service operational cooperation with Israeli officials. We looked into investigations of previous incidents of alleged misuse of Canadian passports, and the advice that the Service had provided to the Government. We noted that the Government of Canada had protested to Israeli officials about the misuse of Canadian passports. Review Committee staff also examined all information exchanges between CSIS and Israeli authorities between 1992 and 1997.

Personal interviews with relevant officials also formed part of our inquiries: these included CSIS officials, Canadian Consular officials, and a senior federal official with the Passport Office. In view of his public comments about the matter, including passport misuse, the Committee also interviewed Canada's former Ambassador to Israel, Mr. Norman Spector.

The Committee's Findings — Main Points

Though CSIS has provided operational assistance to the Israeli officials in the past,

- The Committee found no evidence that CSIS was involved in any manner with the Meshal-Amman incident.
- We found no evidence that Israeli authorities consulted with CSIS about the assassination attempt before the fact.
- We found no evidence (in this incident or ever) of Israeli authorities requesting from CSIS the use of Canadian passports.
- Equally, we found no evidence of CSIS providing Canadian passports to Israeli authorities or turning a blind eye to their use.

Passport Misuse

In our review of CSIS files, we sought out information that would shed light on

whether the Service knew about and then passed to the Government information about the misuse of Canadian passports generally. We found that CSIS had provided comprehensive information to the Government on this issue, had fully investigated all cases of passport misuse by foreign intelligence agencies and, with one exception, had reported to the appropriate agencies of government all instances of suspected passport misuse.

In making queries about the single exception, the Service explained to us that it did not release the information because to do so would have jeopardized third party information from a foreign intelligence service.

With respect to the advice CSIS gave to government in this area, a Director in Canada's Passport Office — the agency of Government with prime responsibility for passport matters — told the Committee that the Service's information had been very helpful and that he knew of no instance in which relevant information had been withheld.

Intelligence "Bartering"

The Committee took note of allegations in the media that CSIS might have provided the Canadian passports or "looked the other way" in return for information from Israeli officials. We found no evidence of such arrangements between Israeli authorities and CSIS in regard to passports or any other inappropriate exchanges.

This conclusion is based on a review of the Service's files, and interviews with CSIS officers and diplomatic officials. Files that predated the *CSIS Act* were examined and retired CSIS officers who would have known about intelligence "bartering" arrangements were sought out and interviewed. None of the allegations were in any way substantiated.

The Committee acknowledges the importance of the "give-get" or *quid pro quo* principle in the intelligence world. However, we can see no substance to it in this case. We came to the conclusion that the story has entered the realm of urban mythology — an oft repeated story with no foundation in fact.

We came to the conclusion that the story has entered the realm of urban mythology — an oft repeated story with no foundation in fact

The Seized Passports — Forged or "Acquired"?

Jordanian authorities gave the two seized passports to Canadian officials. After conducting a technical examination of the passports, RCMP forensic specialists concluded that they were forgeries. The Service's technical specialists then performed their own examination of the two passports and concluded that,

- the passports were counterfeit in their entirety;
- the forgeries were of excellent quality; and
- that given the effort involved, the forgers probably produced the counterfeit passports in large lots.

The Service's information was distributed to the relevant Federal agencies responsible

for passports and for monitoring entry points into the country.

The Nature and Scope of CSIS-Israel Cooperation

In the aftermath to the assassination attempt in Amman, questions were raised in the media as to whether the relationship between CSIS and Israeli officials was restricted to information exchanges, or whether they had cooperated in operational matters.

The term "joint operation" is to be found in the Service's *Operational Policy Manual* and from the Committee's perspective its meaning is ambiguous at best

For the period 1992 through 1995, the Committee identified four matters in which there was cooperation between CSIS and Israeli authorities. We reviewed each of the cases to determine whether CSIS complied with policy, Ministerial Direction and the law. We detected a problem in one case and evident policy ambiguity in another.

Failure to Obtain Independent Confirmation

The first case involved assessments generated by Israeli officials and passed to the Service. In one element of the case, it was evident that CSIS failed to seek out independent confirmation of the shared information. We informed CSIS of our concern about the matter, which involved operational assistance (see below), and recommended to it a course of action.

A Policy Gap

Among the media speculation surrounding the Meshal incident was that CSIS and the Mossad were involved in "joint operations." The term "joint operation" is to be found in the Service's *Operational Policy Manual* and from the Committee's perspective its meaning is ambiguous at best.

This is illustrated by the second case, the only one that went beyond information exchange and approached that of a "joint operation." In it, CSIS provided assistance in Canada to foreign officials that was, the Service states, of an urgent and pressing nature. As such, and according to Ministerial Direction, a CSIS senior executive approved the activity and the Minister was notified after the fact.

The *CSIS Operational Policy Manual* contains provisions for "operational assistance" and "joint operations," and permits senior CSIS personnel to give approval to either form of operational cooperation if the situation is urgent and pressing. The Ministerial Direction, in comparison, states that "operational cooperation" with foreign services must as a rule be approved in advance, and that "operational assistance" can be authorized by senior Service officials in case of urgent and pressing need. The Ministerial Direction is silent on the issue of "joint operations."

It is the Committee's view that in both policy documents a number of key terms employed lack clear definition. The result is an apparent discontinuity between the guidelines in Ministerial Direction and the Service's policy manual which governs the conduct of individual CSIS officers. We believe steps should be taken by the Ministry and the Service to address these policy lacunae.

CSIS Role in Immigration Security Screening

Report #105

Scope and Methodology of the Audit

The main objective of this study was to understand the Service's role in assisting the Government with its Immigration Program and to assess the quality of the relationship between the Service and its interlocutors at Citizenship and Immigration Canada (CIC). Although the review focuses on CSIS' role in providing advice and information to CIC, we also examined that department's priorities and strategies insofar as they impact on the Service's functions. We learned, for example, that in 1998-99, CIC will focus its efforts on enhanced screening efforts at Canada's ports of entry, including offshore and at international airports. Thus, a corresponding increase in CSIS activities in these areas can be anticipated.

To carry out the study, SIRC researchers met with officials from CIC, CSIS, members of the legal community involved in immigration and refugee law from both government and the private sector, as well as representatives of non-governmental organizations working in the field. All relevant CSIS files, interview reports and the briefs sent to CIC were examined. In addition, the Committee conducted on-site audits at three Immigration Case Processing Centers abroad (two in the Middle East and the other in Buffalo, New York). We interviewed an Ambassador and several Immigration Program Managers in order to gain additional insight into the cooperative relationship. The CIC informed us that it views its working relationship with CSIS as extremely good.

The Nature of the Cooperative Relationship

Since the establishment of CSIS, a series of cooperative processes have evolved which define the mechanisms under which the Service assists the country's Immigration monitoring effort:

- the Immigration and Refugee Application for permanent residence (inland and overseas);
- vetting of applications from foreign officials and visitors to Canada;
- enforcement actions (arrest, detention, deportation);
- vetting of individuals claiming refugee status; and
- reviewing applications for citizenship.

Within these programs, the Service's authority for immigration screening is derived from sections 14 and 15 of the *CSIS Act*. The assistance rendered by the Service takes the form of information sharing on matters concerning threats to the security of Canada as defined in section 2 of the *CSIS Act* and advice to CIC in respect to the inadmissibility classes of section 19 of the *Immigration Act*. In addition, the Service carries out immigration screening investigations, including any necessary interviews.

Committee Findings

The cooperative mechanisms for each of the programs noted above are described in some detail elsewhere in this report [see Section 2: Investigation of Complaints,

It is evident to the Committee that the screening process overall is a difficult exercise in risk management

page 62]. The Committee's focus here was to examine activities the Service undertakes to assist CIC that impact on the cooperative relationship generally.

The Increased Use of Electronic Data Processing for Immigration and Refugee Applications

The most visible involvement of the Service in the immigration process is its participation in immigration security screening interviews

With respect to the Service's role in CIC's handling of Immigration and Refugee Applications for Permanent Residence within Canada and abroad, the Committee noted that electronic data exchanges between CIC and CSIS, and the use of pre-established security profiles, considerably reduced the time required for the screening process. Applications for permanent residence initiated from outside Canada — some 80 percent of the total of 215,000 applications — fall under the Overseas Immigration Screening Program. For these, the Service shares responsibility for screening with Immigration officials.

It is evident to the Committee that the screening process overall is a difficult exercise in risk management. There is a constant need to balance security interests against the requirements to fulfill the immigration program's goals in a timely and efficient manner. That the dilemmas associated with prudent management can be especially acute was highlighted in our review of two Middle East immigration posts. Obvious external factors such as geography and the local political situations, and organizational issues such as the capacities of foreign agencies to process the Service's requests for information, all impinge upon the nature of the Service's participation in immigration matters.

The Committee noted that consideration is being given to expanding the technological means currently used to process inland applications to include the processing of applications world wide. The wider adoption of such procedures should facilitate information sharing and at the same time standardize and augment the immigration screening process. We urge CSIS — in cooperation with CIC — to continue to pursue such improvements.

Terminology in a Revised Immigration Act

In the fall of 1996, the Minister of Citizenship and Immigration Canada announced the appointment of an Advisory Group to conduct an independent review of Canada's *Immigration Act*. The Legislative Review Advisory Group working independently from CIC focused on adjustments to legislation and policies that would be required in order to meet the objectives of Canada's immigration policies. Among the recommendations advanced by the Group was a proposal aimed at standardizing terminology across relevant portions of Canadian law. Specifically, they suggested that provisions in any new immigration act referring to an applicant's inadmissibility to Canada on security grounds should be congruent with the definitions of "threats to the security of Canada" contained in the existing *CSIS Act*. The Review Committee fully supports this recommendation.

Immigration Interviews and Screening

The most visible involvement of the Service in the immigration process is its participation in immigration security screening interviews.[3] Typically, arrangements

for the interview are made by CIC and are conducted by regional Security Screening investigators. It is often the case, however, that for various reasons an investigator from one of the Service's other operational branches is also present.

While the Committee is aware of the advantages which accrue from having CSIS section 12 investigators from the regions involved in immigration interviews, their presence does increase the possibility that the interview can be used as an investigative tool, rather than for its intended purpose: to provide an opportunity for the prospective immigrant to explain adverse information in relation to his or her security status. The Committee wishes to underscore the need for CSIS to maintain a balance between the need to provide complete and meaningful advice, and the rights of those being interviewed.

The Committee, however, is also cognizant of the complexities which arise when the prospective immigrant is also the subject of a targeting authority, allowing CSIS to employ interview techniques which are more intensive than those routinely used in immigration interviews.

Immigration interviews in which CSIS investigators participate can only usefully serve as a means to address security-related concerns if the investigators are fully informed and the interviews skillfully conducted. In this respect, the Committee supports an initiative whereby CSIS will be provided with the notes of the relevant immigration officers whenever there is an immigration referral.

In examining the immigration screening process, the Committee reviewed written guidelines to CSIS officers. We found the Service's *Procedures Guidelines on Immigration Screening Interviews* to be inadequate in several respects. The Guidelines currently state that "the investigator should not create the impression that the applicant's cooperation with the Service could facilitate the processing of the application" — a statement we take to refer to the possibility of the applicant's recruitment as a source in the context of a pending application for immigration. In our view, the Guidelines should be less equivocal on the matter and state clearly that immigration interviews will not be used for recruitment or other unrelated purposes. The Service has informed the Committee that the Guidelines are in the process of being updated. We will review the new guidelines to see if this particular concern has been addressed.

The Guidelines should be less equivocal on the matter and state clearly that immigration interviews will not be used for recruitment or other unrelated purposes

In addition, the Committee is of the view that the screening process would benefit from an explicit reference in the Service's *Procedures Guidelines* to section 8(1) of the *Immigration Act*. Here it states that an applicant who seeks entry to Canada bears the burden of proving that he or she is entitled to enter this country, and that such entry would not contravene the *Act* or the other regulations. All applicants for entry into the country should be aware that non-cooperation with the screening process will prevent their applications from being processed.

The Committee is also aware, however, that in all but exceptional circumstances,

applicants are unable to address particular concerns until they are in possession of sufficient information about what is alleged. We believe that every effort should be made by CSIS within the obvious security constraints to release the maximum amount of information to the prospective immigrant. Our review of Service briefs to CIC identified ongoing efforts toward this end.

We believe that the Service's investigative expertise could be useful in interviewing applicants suspected of war crimes

Finally, with respect to CSIS briefs, our research found that some reports contained information derived from the CSIS computerized data base and open information. It is the Committee's view that reports on immigration interviews should contain only information collected during the interviews or, failing that, be unambiguous about what was or was not discussed at that time. In reading the reports, it was sometimes difficult to distinguish between what was said by the applicant, what was said by the interviewers to the applicant, or whether the information was from other sources altogether.

CIC's "War Crimes Strategy"

The Committee is aware that one of CIC's priorities is to strengthen Canada's ability to detect applicants suspected of war crimes or crimes against humanity. In view of the fact that the RCMP does not currently assist CIC in the conduct of screening interviews, we believe that the Service's investigative expertise could be useful in interviewing applicants suspected of war crimes. The Service maintains that as a matter of routine, it passes to CIC any war crimes-related information it obtains. The Committee believes that the Service's responsibilities in this area should be formalized and set out in policy.

Service Assistance in Enforcement and Interdiction

The Service participates in the recently established Points of Entry Interdiction Program of CIC. The role of CSIS is to provide advice in an expeditious manner to CIC on whether a particular individual wishing to gain entry poses a threat to the security of Canada. Immigration officials take this advice into account when making a determination about the eligibility of an applicant under section 19 of the *Immigration Act*. Until June 1998, the Service did not document or record these opinions. However, since then, CSIS documents all interdiction interviews it participates in. The information is held in the section 15 Security Screening Information System (SSIS), and is comprised of the subject's biodata as well as a reference to whether a report was submitted to the section 12 operational data base. Notwithstanding this procedure,

> We recommend that, in future, all advice given to CIC should be recorded, along with the specific details about the individual interviewed.

CSIS and Individuals Claiming Refugee Status

Of the nearly 26,000 refugee claims made in Canada in 1997-98, 60 percent were made at border points and the remainder at Immigration offices inland. When a person claims refugee status, senior immigration officers question the individual and request that a personal identification form (PIF) be completed. Officials then examine all of the available relevant documentation, such as passports, other identification, and travel

documents. The officers also photograph the claimant and take fingerprints. The fingerprints are forwarded by mail to the RCMP to ascertain whether there is another claim on file with the same fingerprints, and whether the claimant has a criminal record in Canada.

It is evident to the Committee that there are flaws in this process. In a review of refugee handling procedures, the Auditor General wrote that in most cases immigration officers rule on the eligibility of a claim without first obtaining the information required to make an informed decision.[4] Thus the evaluation of eligibility is essentially based on the claimant's statement.

The Committee's review also shows that before the refugee hearings are held, the refugee claimants' names are not, as a matter of course, screened against the data banks held by the Service. As we understand the original rationale behind the decision to proceed in this manner, immigration officials did not regard the screening of all refugee applications as a productive activity since at the time only 20 percent were approved by the Immigration and Refugee Board (IRB), and in any event, most were in Canada for a maximum of six months.

The situation with respect to refugee claimants is now substantially different. Since 1993, the overwhelming majority (99 percent) of refugee claimants have been ruled as eligible to seek refugee status, and an individual claiming refugee status can count on staying in Canada for much longer before a final decision is made. In recent years, close to 60 percent of claimants have presented themselves to Canadian officials without a passport, personal identification, or travel documents.

It is the Committee's view that in this quite different and much more demanding context, CIC needs to know as much as possible about would-be refugees as it pertains to threats to Canada's security interests. Claimants' backgrounds in Canada and abroad need to be known and understood, and we are convinced that CSIS has an appropriate role to play in this process.[5] Although CSIS is currently not involved in screening refugee applicants, there are ongoing discussions with CIC on this matter.

The Committee believes that CSIS should play a greater role in refugee matters, but that role should be carefully defined and transparent

CSIS already provides some information about refugees to CIC. We have noted, for example, several instances when individuals with refugee claims have appeared before the Immigration and Refugee Board, the CIC has opposed their claim employing information obtained from CSIS, and the IRB has subpoenaed Service officers to testify about information provided through affidavits. The Committee believes that CSIS should play a greater role in refugee matters, but that role should be carefully defined and transparent.

Complaints About Immigration Screening

The Committee is charged with the investigation of any complaints stemming from immigration screening interviews. We anticipate that they will provide the Committee with even greater insight into the Service's immigration role, and how the system functions in terms of legislation, policy and fairness. The first hearing of

such complaints is scheduled for July 1998. Others will be heard in September 1998.

A Foreign Conflict

Report #96

The Committee examined a set of CSIS investigations of groups and individuals implicated in an armed conflict in a foreign country. The purpose of our review was to determine whether the Service's investigations were appropriate in light of the threat posed by the targets chosen; and were conducted in accordance with the *Act*, Ministerial Direction and established CSIS policies and procedures.

Methodology of the Review

Our review covered the period from April 1995 through March 1997, and was focused on the Service's investigation of a well-known terrorist group and a small number of individuals. Examined by Committee researchers were all hard-copy and electronic files pertaining to the selected investigations as well as the advice provided to Government arising from them. The information compiled by the Service was both voluminous and varied. The materials we reviewed included:

- targeting submissions and authorizations;
- interviews with individuals linked to the terrorist group in question;
- evaluations of the threat posed involving international gatherings (for example the 1995 G-7 Economic Summit held in Canada), visits to Canada by foreign VIPs, and possible reprisals against certain embassies in Canada;
- reports from sources;
- information from foreign intelligence services or CSIS reports prepared from that information; and
- monthly reports on terrorism issues prepared by the Counter Terrorism Branch at Headquarters.

Background to the Service's Investigations

According to CSIS, a relatively small group of Canadians, landed immigrants, and refugees in Canada support or, at the very least, sympathize with the terrorist group in question. Some of these sympathizers have fled a checkered past to seek refuge in Canada, which serves as a staging and coordination area for terrorist operations elsewhere.

CSIS and the Use of Surveillance

CSIS uses surveillance to learn about the behaviour patterns, associations, movements, and "trade-craft" of groups or persons targeted for investigation. As an investigative tool, surveillance is used to detect espionage, terrorism, or other threats to national security. Large amounts of personal information can be collected and retained in the course of surveillance operations. The Service's surveillance units use various techniques to gather information. In an emergency, surveillance can be used before a targeting authority has been obtained.

The Service regarded the potential of the threat posed as especially serious in light of the particular combination of attributes possessed by the targets:

- certain of the extremists investigated have not sworn allegiance to any one group, but instead maintain relations at the highest levels with a number of terrorist organizations;
- some of the individuals targeted, although nationals of one country, take orders from or give direction to extremists of a number of other nationalities; and,
- certain of the extremists connected to the investigations are involved in multiple foreign conflicts at any given time.

Given the international dimensions of the investigations, CSIS concluded detailed intelligence-sharing agreements with a number of foreign intelligence services with which it maintains ongoing links. The exchange of information focused on three areas: international extremist movements; the role of certain organizations which were believed to provide documents, recruit activists, and support terrorist acts; and methods of communication between extremist groups and members.

The Committee's Findings

Based on our review, we came to the conclusion that in respect of this set of investigations, CSIS had in its possession sufficient information to warrant the targeting, and that in general, it conducted the investigation in accordance with the *Act* and its operational policies. We identified a number of facts and events which pointed clearly to direct threats to Canada's national security interests including, threats to life and limb of Canadian diplomats posted overseas and the possibility of a bomb attack in Canada.

The Committee took especially serious note of information provided to CSIS to the effect that a Canadian citizen was involved in a conspiracy to assassinate a politician in a foreign country. CSIS also learned that the individual was allegedly linked to several criminal activities inside Canada. When the Service's investigators witnessed criminal activities committed by the individual and accomplices, the police force of jurisdiction was duly informed.

This same individual attracted a great deal of interest overseas, resulting in numerous exchanges of information between CSIS and the intelligence services of other countries. The extent of these exchanges varied greatly. One country's service appeared impatient with the manner in which CSIS was supplying the requested information, and there was some friction between security services of another state and CSIS over a difference of opinion about the seriousness of the threat posed by another individual. It was evident to the Committee that these strains abated in the wake of the Service's continuation of its investigations.

While we were satisfied overall with the appropriateness of the Service's intelligence collection arising from the investigations, the Committee identified three operational reports on an individual's personal life that did not, in our view, meet the criterion of being "strictly necessary" as set out in section 12 of the *CSIS Act*. The Committee

The Service regarded the potential of the threat posed as especially serious in light of the particular combination of attributes possessed by the targets

recommended that the Service delete them from its data base and the Service has done so.

Coordination of Government Economic Security Efforts — the Service's Role

Report #92

The Committee's 1996-97 review of the CSIS economic espionage investigations revealed relatively little formal cooperation and coordination between CSIS and other government departments on economic security issues.[6] We also concluded that for CSIS to conduct meaningful investigations of threats posed by economic espionage, it would need to have access to additional technical and business-related expertise.

For this year's audit report, we sought answers to three questions: what mechanisms for coordination on matters of economic security among government departments and agencies were in place, what was the nature of the Service's participation, and what impact did these mechanisms have on CSIS investigations. Our inquiries for the audit covered Ministerial Direction given to CSIS and the Service's administrative cooperation files. The Committee also conducted interviews with staff in the Economic Security and Proliferation Issues (ESPI) Unit at CSIS Headquarters.

Current Cooperation and Coordination Mechanisms

ESPI has two specific areas of investigative responsibility: the threat of economic espionage directed against Canadian national interests, and the proliferation of weapons of mass destruction. Our most recent review showed that while ESPI has not been asked to participate in any formal coordination body in the economic security area, it does consult with and engage in joint presentations with other Federal Government departments and agencies, as well as liaise with law enforcement bodies.

We noted that ESPI refers clients to other agencies that are expert where the Service is not. In the course of Liaison/Awareness

Background to CSIS Economic Security Program

The changing international threat environment of the post-Cold War world has pushed economics to the top of the national intelligence agendas of many countries, Canada not excluded. The Government of Canada has broadened its definition of national security to include the concept of "economic security" which CSIS defines as "the [set of] conditions necessary to sustain a competitive international position, provide productive employment, and contain inflation."

Reflecting these changes in the nature of the challenges to Canadian security, the Service initiated in June 1991 a comprehensive approach to two issues: "Economic Security" and the "Proliferation of Weapons of Mass Destruction". In order to co-ordinate the existing organizational sections within CSIS investigating these areas, the Service formed the Requirements Technology Transfer (RTT) Unit.

presentations, for example, the Service was sometimes asked by private sector contacts for more information on how they could ensure that their information systems were secure. In such cases, CSIS would refer the inquiries to the Communications Security Establishment.

The Service's product in the economic security area is directed to a wide range of domestic Federal Government clients, based on their needs. Among these clients is the Intelligence Assessment Committee (IAC) of the Privy Council Office (PCO). The IAC coordinates and facilitates interdepartmental cooperation in preparing analytical and assessment reports for Ministers and senior government officials.[7] CSIS participates in the process upon request by preparing reports for the IAC, though our review indicated that on issues of economic security, the requests are few and far between. CSIS contributions to the area have been on an *ad hoc* basis and mostly in the form of inter-departmental committee discussions. The Service has also provided intelligence on a bilateral basis to other departments, as well as through the production of intelligence assessments shared with domestic clients.

Committee Findings

In its 1996-97 Report, the Committee suggested that the Service could better fulfill its mandate in the area of economic security by making more use of technological and business-related expertise. One source of such information lies in other areas of Government. It is apparent to the Committee, based on this most recent review, that the dearth of coordination and cooperation between Government agencies is a reflection not of the Service's efforts, but of what appears to be the relatively low priority the Government of Canada as a whole gives to the issue. The development and maintenance of any formal cooperation process within government is a complex undertaking contingent upon the priorities and resources of the various government departments involved. The Service showed itself to be a capable and willing participant in the coordinating mechanisms that do exist, but these bodies devote relatively little effort to economic espionage matters.

The Service showed itself to be a capable and willing participant in the coordinating mechanisms that do exist, but these bodies devote relatively little effort to economic espionage matters

When our previous study found little ongoing cooperation with other government departments and agencies, we were concerned about the impact on the Service's economic security investigations. Notwithstanding the low priority apparently assigned to the subject by other agencies, the Service has said that its economic security investigations were not adversely affected by the lack of coordination in the area. Our review identified no evidence to dispute the Service's conclusion.

On the basis of both the 1997 and 1998 studies, we concluded that the Service has not devoted much in the way of resources to economic espionage investigations but that other sectors of Government appear to regard matters of economic security as having an even lower priority than does CSIS. It was also our view that the Service's definition of economic security encompassed more issues than many would agree are vital to Canada's security, that strong evidence of foreign government interference was elusive, and that some of the information the Service had collected

was not specifically linked to threats to the security of Canada.

In summary, we believe that the Service should clarify its definition of economic security in order to better focus its investigations and avoid the problems outlined above. This Committee sees CSIS as being limited by its mandate to the investigation of state-run intelligence agencies and their proxies in this area. We believe that the focus is not strictly on economic security, but rather foreign interference in Canadian society. If the Government of Canada wishes CSIS to go beyond this, it should introduce amendments to the legislation. We have been informed that the Service is comfortable with the direction it has received from the Government on this issue.

It was also our view that the Service's definition of economic security encompassed more issues than many would agree are vital to Canada's security

Exchanges of Information with Domestic Agencies

Report #95

In the course of discharging its mandate to investigate suspected threats to the security of Canada, CSIS exchanges information and intelligence with other Canadian government departments and police forces. The *CSIS Act* specifically provides for the Review Committee to examine both the exchange and cooperation agreements the Service has with other agencies, as well as the information and intelligence shared.[8] As a matter of practice, the Committee examines most CSIS exchanges of information on an annual basis, and evaluates the effectiveness of Service cooperation in two regional offices.

Methodology of the Evaluation

In sorting through literally thousands of information exchanges, the Committee looks for those that exceed the Service's mandate or are unnecessary. The goal is to assure ourselves that CSIS has the authority both to provide the information it shares with others and collect the intelligence others provide to it. We also review the content of the exchanges to determine whether personal privacy has been violated, and to ensure that the nature and scale of the information is proportional to the alleged threat posed by the individual.

An additional and equally important aim of our review is to assess the quantity and quality of inter-governmental cooperation at CSIS regional offices: has the Service adhered to the guidelines set out in its arrangements with other institutions; is it in compliance with the *CSIS Act*, with its own policies and procedures with respect to disclosure and liaison, and with Ministerial Direction.

Committee Findings

This year's domestic exchange report is unusual in that cooperation issues dominated our findings. In the two regional offices visited, we focused our review on the status of CSIS cooperation with other federal and provincial agencies.

CSIS and Law Enforcement Relations

Both CSIS regional offices we audited were experiencing difficulties in their relations with a particular law enforcement agency with respect to certain investigations. In one CSIS region, relations with a police agency were at an extremely low ebb during our audit because of a legal action underway at

that time. In view of the fact that the specific issue is the subject of a separate Committee review, we did not pursue the case in this audit. [See "A Problematic Case of Inter-agency Cooperation", page 32].

We did, however, inquire generally into the Region's problematic relationship. The CSIS Regional office stated that its operations had not been significantly affected by the legal case, and that in any event, the law enforcement agency in question was not central to Service investigations in the region. Our review of the region's information exchanges confirmed that the Service's primary law enforcement relationship was with another police agency, where relations continue to be excellent.

In the second region, the problem concerned an investigation against a target that the Service and the police had conducted in parallel. The Service was unhappy that it had not been given more access to police information and intelligence on the case, reflecting differences of opinion generally between the agencies over access to each other's information. We were assured by the regional office that the disagreements had not affected other investigations.

The Committee was unable in the time permitted to determine all of the factors contributing to the tensions between CSIS and the police. We believe that the relationship between the organizations warrants closer examination and a study focused on the issue is underway. One early conclusion we were able to draw from the current review is that conflict between the Service's requirement to protect its sources and the law enforcement need to use CSIS information in judicial proceedings is a source of tension. At the heart of this issue is the 1991 Supreme Court of Canada decision in R. v. Stinchcombe. [See the inset on the Stinchcombe ruling, page 31]

The issue of judicial disclosure weighs most heavily on CSIS counter terrorism investigations. The Review Committee will continue to monitor the impact — if any — of judicial disclosure on national security operations.

Conflict between the Service's requirement to protect its sources and the law enforcement need to use CSIS information in judicial proceedings is a source of tension

CSIS Cooperation with Citizenship and Immigration at Points of Entry

The Committee has taken note of a new initiative in which CSIS has undertaken to work with other federal agencies to improve existing procedures in regard to the interdiction at points of entry into the country of individuals known to be threats to Canada's security. Called the Point of Entry Alert Program (POEAP), an evaluation of it forms part of the Committee's review of immigration screening beginning at page 9 of this report.

CSIS Denied Access to Provincial Government's Information

The Committee's review identified a case where CSIS was refused access to information held by a ministry of a provincial government. Under the agency's interpretation of the province's privacy legislation, CSIS did not qualify as a "law enforcement body" and thus could not receive the information. CSIS suggested a number of options that would be consistent with the province's laws and still permit the sharing of appropriate information with the ministry in question. The Service also stated that it was still able

The Committee's review identified a case where CSIS was refused access to information held by a ministry of a provincial government

to access information from other agencies in the province under another provision of the same law. On the Review Committee's part, we had concerns about the inconsistent application of the law inherent in such a position and queried whether the Service could continue to have access to information held by any government body in the province. After reviewing the matter, we concluded that we did not take issue with the Service continuing to negotiate access with each ministry, as long as the latter had the statutory authority to release the information.

Exchanges Outside the Mandate

Three information exchanges between CSIS regional offices with other government agencies drew the Committee's attention. In the first, CSIS had received and retained section 12 ("threats to Canada") information in the absence of a targeting authority. We agreed with the Service's explanation that the reports were unsolicited and fell within the Service's mandate. In the second, we identified information CSIS had received from another agency that we believed was outside the Service's mandate to collect. And with respect to the third exchange, the nature of the information led us to question the Service's authority to pass on the information it had collected to a particular agency.

New Policies and Ministerial Direction for Information Exchange

CSIS has signed no new arrangements with other government agencies since 1996 and the Minister issued no Direction that would have impacted on the Service's exchanges of information and cooperation. We noted that the Service initiated new operational policy involving on-going cooperation with another federal government agency.

CSIS Liaison with Foreign Agencies

Report #98

Methodology of the Audit

Under section 38(a)(iii) of the *CSIS Act*, the Committee reviews the foreign arrangements entered into by CSIS with foreign police and intelligence agencies, and monitors the flow of information to agencies with which CSIS has arrangements.

This year, we examined two posts that are instrumental to the Service in its collection of information concerning extremism. The review encompassed the following material:

- all exchanges of information handled by the CSIS Security Liaison Officers (SLOs) at the two posts, including electronic exchanges;
- all correspondence with the foreign intelligence agencies handled by the posts; and
- all instructions and reference materials provided to and by the SLOs, including "Assessments of Foreign Agencies".

Our audit involved on-site visits to examine files and to conduct interviews with SLO personnel and others. At CSIS Headquarters, we reviewed the impact of the reorganization of the section responsible for foreign liaison, and the new logging system put in

place to track exchanges of information with foreign agencies.

Reorganization of Foreign Liaison Within the Service

As discussed in last year's audit report (page 4) CSIS recognized the increasingly important role of foreign liaison in security and intelligence operations by upgrading the Foreign Liaison and Visits Section to Branch status with a Director General-level appointment as its head.

In the course of the Committee's audit of the posts, two issues of relevance to the recent headquarters reorganization arose that we believe merit highlighting.

Need for Centralized Tasking Authority

The SLOs we interviewed underlined the need for increased coordination and monitoring of requests and tasking from CSIS Headquarters. Under current practice, each operational branch of CSIS tasks SLOs directly, creating sometimes competing and conflicting demands for SLO resources. Future reviews will focus on this issue.

Correspondence Tracking System

The second issue concerned the system (recently introduced) to track correspondence at the Service's posts abroad. In the Fall of 1997, all SLO posts' systems for logging electronic exchanges were upgraded to a system called the Correspondence Control Management (CCM) program. The Committee had noted in previous audit reports that the tracking system then in place was flawed. We are pleased that CCM appears to have alleviated the earlier audit difficulties.

Activities of Security Liaison Officers

CSIS Security Liaison Officers are stationed abroad to maintain and develop relationships with foreign agencies, to conduct security screening procedures, to report events and developments of Canadian security interest, and to assist Mission Security Officers resident in Canadian diplomatic missions abroad. They meet formally and informally with the representatives of foreign police and intelligence agencies. The Committee reviewed the SLOs' actions and activities and identified a number of problems.

Canadian Residents Traveling Abroad

In examining the requests for specific information made to SLOs from foreign agencies we identified situations where the policy guidelines governing SLO conduct were silent when it came to certain kinds of requests. For example, CSIS can ask foreign intelligence services to monitor Canadian residents who travel to other countries. We recently examined several such cases.

> We recommend that CSIS develop policy regarding requests for assistance to foreign agencies to investigate Canadian residents traveling abroad.

An Appearance of Offensive Intelligence Gathering

In the absence of an authorization from CSIS Headquarters, an SLO conducted inquiries of foreign intelligence officers about a terrorist who it was believed might attempt to enter Canada. Under existing policy and law, SLOs have no mandate to conduct investigations outside of Canada

We identified situations where the policy guidelines governing SLO conduct were silent when it came to certain kinds of requests

and must refrain from any activity that gives the appearance of offensive intelligence gathering. We have raised the case with the Service.

Agency Assessments

In order to assist CSIS generally to decide what types of information and intelligence can be released to foreign agencies, SLOs are charged with the responsibility of preparing "agency assessments" that comment on the reliability and human rights records of foreign police and intelligence services with whom they interact. For the two posts at issue, we found that the SLOs' assessments were accurate and appropriate, especially as they pertained to the prevailing human rights situations.

SLOs' assessments were accurate and appropriate, especially as they pertained to the prevailing human rights situations

Exchanges of Information

CSIS is able to exchange information with foreign agencies via several channels: visits of officials, through SLOs stationed abroad, and by direct electronic link. Review Committee staff examine the records of all these exchanges.

Information Exchanges Involving Individuals at Risk

One of the Committee's concerns is that information the Service shares with others does not put individuals at undue risk from foreign security services. At one post, while we observed a significant volume of exchanges concerning individuals, we also noted that CSIS reports did not identify persons in Canada, and instead focused on leaders of extremist groups rather than on rank-and-file members and supporters.

At the second overseas post, CSIS had requested trace checks from foreign agencies on a significant number of persons, and in a few cases, had made available detailed information from Canada-based investigations. The Committee found no evidence that the releases were excessive, or that the releases had resulted in harm to any person.

Inappropriate Information Sharing

The Committee identified an instance where the Service's sharing of information with a foreign intelligence service was questionable. CSIS handled a request from a Canadian law enforcement agency to ask several allied intelligence services to conduct records checks on more than 100 people suspected of being involved in transnational crime. The Committee found the grounds for some of the requests to be of doubtful validity. For example, one person about whom information was requested was said to have been "caught shoplifting."

We noted that the Solicitor General during the year under review issued a new Ministerial Direction whereby CSIS was directed to facilitate the relaying of transnational crime information from foreign intelligence and security services to the appropriate Canadian law enforcement agencies.

Foreign Liaison Arrangements

Under section 17 of the *CSIS Act* the Service, with the approval of the Solicitor General, can enter into an arrangement with a foreign agency. CSIS has some 212 such agreements with foreign police and intelligence services, many of which predate the *CSIS Act*. In 1985, following the establishment of CSIS, these arrangements were

deemed to be in effect (or "grandfathered") when the Solicitor General of the day approved them. The Committee's audit of the two overseas posts shed light on a number of policy issues having to do with CSIS liaison relationships generally.

Cooperation with a Foreign Agency for Which No Agreement Can Be Found

The Ministry of the Solicitor General produced in 1985 a compendium of CSIS arrangements with foreign governments and institutions comprising the Ministry's "understanding of all arrangements presently in place between the Canadian Security Intelligence Service and foreign governments or institutions of governments." However, in the case of one foreign intelligence service with which the Service has an on-going relationship, we could find no document to show that an arrangement for security intelligence exchanges existed prior to 1984. We have notified CSIS of this discrepancy.

Reactivating Dormant Arrangements

In the course of our review, the Committee took note of a case where a foreign arrangement had been dormant for ten or more years, and then was reactivated. During the dormant period, however, the political environment of the country concerned had changed substantially. In examining the reactivation, the Committee found that while an informal, local consultation process occurred, there was no formal procedure in place to review the new circumstances. We also determined that there was no provision in CSIS policy or Ministerial Direction that would require CSIS senior management or the Minister — prior to any reactivation — to revisit the terms and conditions of an arrangement made under quite different circumstances.

> We recommend that CSIS policy be revised so as to ensure that the terms and conditions of foreign arrangements that have been dormant for a significant period of time are revisited before reactivation.

Two Instances of Cooperation Outside the Terms of the Arrangement

The Committee identified a case wherein CSIS had discussed with a foreign intelligence agency several proposals for intelligence operations which the Committee believed were outside the mandate of the existing arrangement. The scope of the arrangement suggested to us that the planning activity undertaken in fact required Ministerial approval. The Service, on the other hand, interpreted the arrangement differently, asserting that the existing agreement did cover the discussions preceding operational activity. Although the operations were not in the end carried through and did not proceed beyond preliminary planning, we believe that CSIS policy and Ministerial Direction should re-address this issue so as to remove any ambiguity.

In another case, a foreign government required that information exchanged by all of its agencies flow through its intelligence service on the way to its eventual destination. With respect to immigration and security screening information, however, the Service's arrangements were with a separate agency in the same country. CSIS followed the foreign government's direction thus causing

The Committee's audit of the two overseas posts shed light on a number of policy issues having to do with CSIS liaison relationships generally

CSIS immigration and security information to be shared with an agency with which it had no appropriate agreement.

In light of the circumstances we observed, the Committee came to the view that the practice was inappropriate and so notified the Service. The Committee subsequently learned that CSIS had taken steps to regularize the situation by seeking the authority to alter its arrangements such that immigration and security screening information could be shared with the intelligence service concerned.

Implications for Foreign Liaison Policy

CSIS foreign arrangements are governed by a 1982 Ministerial Direction that predates the 1984 *CSIS Act* and employs terminology and describes administrative procedures that are not consistent with the *Act*. Less obviously, many of the definitions and

Background to the Service's Foreign Liaison Program

From the inception of CSIS in July 1984, until 1989, CSIS had a Foreign Liaison Branch. In 1990, the Service replaced the Branch with a new system for communicating with and coordinating the efforts of the SLOs. At the time, SIRC expressed its concern about the disbanding of the Foreign Liaison Branch. The Committee regretted the loss of what it described as "An intermediary... [that could] 'blow the whistle' on the inappropriate dissemination of information abroad."[9]

In its place, CSIS created a new unit under a Coordinator, to provide administration and support services to the SLOs. The Coordinator reported to one CSIS executive member, while the SLOs reported directly to another. The Foreign Liaison Advisors reported to their respective operational branches, and were to monitor the correspondence exchanges and ensure that the SLOs were informed about new developments.

In a previous Annual Report,[10] we expressed concern about the number of SLO posts CSIS was closing and were of the opinion that, "the foreign liaison program would benefit from more attention from the Service, not less, as seems to be the trend in terms of representation overseas."

For a number of years, there were few changes to the Service's posts abroad, save for the post closings, but the mid-1990s saw a major reworking of the Service's foreign liaison strategy. Decisions to open as well as close selected Security Liaison Officer posts resulted, as did changes to the management structure of the foreign liaison program as a whole.

In 1994-95, the reporting relationships and responsibilities changed for both the section and the SLOs, as a result of an internal management study. Most notably, the overall management of the program was once again managed under the direction of a senior manager. In 1997, the program was raised to the status of a branch, headed by a Director General. As noted in last year's audit report, the Committee presents this year an evaluation of SLO activities under the new regime.

terms in the Direction are confusing and contradictory; this is particularly true of the definitions of scope which are ambiguous as to when the Minister must be consulted or advised. Compounding the problem is the fact that Service policies in the area are drawn from this early Direction.

For these reasons, the Committee wishes to repeat the hope expressed in last year's Annual Report that forthcoming Ministerial Direction, which is intended to replace the 1982 Ministerial Direction, will describe foreign arrangements in consistent and comparable terms, understandable by all elements of Canada's intelligence community.

A Comprehensive Review of Foreign Arrangements

Fully one-half of the Service's 212 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS and, of these, many pre-date even the 1982 Ministerial Direction. The Committee is aware of Service procedures to report on certain arrangements annually, on a local basis. However, we have in past audits identified reports that favorably rated disreputable agencies, and we remarked on arrangements that had been left dormant for many years.

The Committee is cognizant of the need for CSIS to enter into new arrangements and build on existing ones with a view to enhancing Canada's national security interests. We believe that the imminent release of new Ministerial Direction will also provide the opportunity to ensure that all foreign arrangements, particularly those that pre-date the Service, are reassessed and annotated so as to bring them into compliance with the new Ministerial Direction and the *CSIS Act*.

> We recommend that CSIS systematically reexamine all foreign arrangements after the release of the new Ministerial Direction on foreign arrangements.

The Committee also recognizes that a reexamination of foreign arrangements in the manner we suggest has significant resource implications and will require a number of years to complete.

Fully one-half of the Service's 212 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS

Investigations of Domestic Threats

Report #100

The Committee reviewed several investigations CSIS conducted during fiscal year 1996-97 which involved threats that were domestic in origin. One investigation was issue-based, while the others focused on groups and individuals suspected of posing a threat of serious political violence as defined in sections 12 and 2(c) of the *CSIS Act*.

Findings of the Committee

We concluded that in almost all the cases we examined, the investigations met these criteria and were conducted in accordance with Ministerial Direction and established CSIS policy. Suspicions about the targeted persons and groups were well-founded; the targeting level selected for each investigation was proportionate to the threat; and, in

almost all instances, the information the Service collected and retained met the test of being "strictly necessary" for the Service to be able to ascertain the nature of the threat posed.

The Committee did, however, identify a few Service reports containing information which, in our view, did not meet the "strictly necessary" standard. The Committee recommended that the Service remove this information — which pertained to sexual orientation and psychological distress — from its data banks. The Service has done so.

We also reviewed an affidavit for warrant powers, and the advice that CSIS provided to the Government on the investigations. We concluded that the information in these documents reflected accurately, and in a balanced manner, the data and the facts collected by CSIS, and that the assessment of the potential threat was justified.

Auditing CSIS Investigations

In the course of reviewing investigations conducted by the Service, the Committee has access to and examines any and all Ministerial Direction, hard-copy and electronic files collected, as well as the Service's advice to Government in respect of the investigations. The Committee seeks answers to four central questions:

- Were there were reasonable grounds to suspect a threat to Canada's public safety and national security as defined by sections 12 and 2(c) of the *CSIS Act*;
- Were the levels of the investigations proportionate to the alleged threat;
- Was the information CSIS collected strictly necessary; and
- Did the advice the Service gave to the Government accurately reflect the intelligence it collected.

CSIS Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada" which it is specifically charged to investigate include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state..." [section 2(c), *CSIS Act*]

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in the denial of citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

CSIS Cooperation with the Royal Canadian Mounted Police - Part I

Report #101

In its investigation of suspected threats to the security of Canada, CSIS cooperates and exchanges information with Canadian government departments and police forces. The nature of the cooperation is usually set out in a formal agreement between the Service and the other agency. With regard to these arrangements, the Review Committee has a responsibility to examine all agreements and to monitor the provision of information and intelligence covered by them.

This year, we focused our attention on the Service's cooperation with the Royal Canadian Mounted Police (RCMP). The nature of the cooperative relationship between CSIS and the RCMP is of particular salience because the RCMP is a significant user of the Service's product and because the RCMP provides information and intelligence to the Service. And, of course, both organizations are essential components of the system which protects the security of Canada and Canadians.

In accordance with its responsibilities as set out in the *CSIS Act*, the Service may provide to the relevant police authority — municipal, provincial, or national (the RCMP) — information that may come into its possession concerning possible criminal activities. In embarking on a study of the CSIS-RCMP relationship, the Committee's interest was not only in this standing general responsibility, but as well, in the process by which CSIS and the RCMP exchange information about activities at the core of each of their mandates: CSIS to *collect and disseminate* information about threats to Canada and the RCMP to perform necessary *police functions* in relation to those same threats.

The responsibilities of each agency are set out in general form in the *CSIS Act*, the *RCMP Act* and the *Security Offenses Act*. Pursuant to subsection 17(1)(a) of the *CSIS Act*, the means and methods of cooperation are elaborated upon more specifically in an agreement between the two agencies. This Memorandum of Understanding (MOU), completed in 1990, is an expression of the Government's expectations in the area of RCMP-CSIS relations and provides the basis for all cooperation and liaison activities between them. In reviewing CSIS-RCMP cooperation, the Committee's goal was to identify any systemic problems in the relationship that would impact upon the ability of either agency to fulfill these expectations and execute the responsibilities each has in security-related matters.

The nature of the cooperative relationship between CSIS and the RCMP is of particular salience because the RCMP is a significant user of the Service's product

Undertaking the Review

The Committee's attention to the area was drawn by recent Committee reviews which revealed several instances of difficulty and disagreement in the CSIS-RCMP relationship. We wanted to determine the extent of the problem with a view to suggesting how cooperation could be improved in order to better protect Canada's national security interests.

In embarking on the study, the Committee believed that the contrasting organizational structures of the two agencies could become

We wanted to determine the extent of the problem with a view to suggesting how cooperation could be improved in order to better protect Canada's national security interests

a significant factor in any findings we might make about operational cooperation between the two agencies. CSIS is highly centralized, whereas the RCMP's operational structure is relatively dispersed and decentralized. It is inevitable, therefore, that some issues which arise first at the regional level are discussed and resolved between the agencies' respective headquarters.

Consequently, we structured our inquiry to proceed in two stages: the first, summarized in the current audit report, examines the state of relations between the two agencies at the headquarters level. It is to be followed at a later date by a review of relations at the regional and field office levels. As a result of this "two-stage" approach to the audit, we will draw most of our conclusions and set out recommendations, if any, at the completion of the second stage which we will report on in our next audit report.

Methodology of the Audit

The relationship between the Service and the RCMP is intensive and broadly-based. Both are heavy users of the other's information and intelligence, and the formal agreement between them provides for an extensive exchange on operational matters relevant to the other's responsibilities. Both agencies operate across Canada, and there is direct liaison and operational cooperation in the regions as well as at the respective national headquarters in Ottawa. In addition to operational matters, the agreement provides for considerable cooperation on non-opertional matters which is handled mainly at the national headquarters level.

Our review covered the first eight months of 1997, though we found that in some cases, events both before and after that period had to be taken into consideration to ensure balanced and objective conclusions. Material reviewed for the audit included CSIS hard-copy administrative files and its relevant computerized data base. Interviews were conducted with the Service's RCMP Liaison Officer, other senior CSIS officers, and their counterparts in the RCMP.

The Nature of Existing Liaison Arrangements

Consistent with the agreement between the Service and the RCMP, both have agreed upon and have established mechanisms to facilitate liaison and cooperation. These mechanisms are centrally managed at both headquarters and include the assignment of personnel to a liaison role at the regional level as well as at the national headquarters of the two agencies.

The liaison officials also act as a primary channel for the exchange of operational information and intelligence. They are given *conditional* access to material and information which their host agency regards as potentially relevant to the other's security-related responsibilities. The access is conditional in that the generating agency must decide whether to accede to the liaison officers' requests for further disclosure to, or use of the information by, the other agency. Under these procedures, it is intended that liaison personnel act to identify information of potential use to their own agency. In addition, certain other forms of information and intelligence on specific matters mentioned in the MOU

are routinely exchanged via direct agency-to-agency channels.

Results of the Review

Overall, the Committee concluded that the existing liaison mechanisms have had a significant positive impact on the relations between the RCMP and the Service, particularly in providing a better mutual understanding at all levels of respective roles and responsibilities. We observed cooperation initiatives being actively supported and promoted by the senior management at the headquarters of both agencies, and can also conclude that for the most part, the existing liaison mechanisms serve to identify developing problems at an early stage.

With respect to the non-operational areas of cooperation — much of which does not go through designated liaison officers but instead involves long-standing exchange arrangements conducted on an HQ to HQ basis — we observed no difficulties of consequence.

Problems in the Use of Operational Information Exchanged

Conflicting Responsibilities and Disclosure to the Courts

While the mechanism for the basic exchange of information appears sound, the Committee did identify areas of difficulty with respect to decisions by CSIS about which information is to be disclosed and how it is to be used by the RCMP. These problems arise when the responsibilities and interests of both parties conflict in respect of CSIS operational information to which RCMP liaison officers have been given access.

The primary role of the Service is to collect intelligence on threats to the security of Canada, using sources and investigative methods which must be protected in the interests of national security. The intelligence collected is not intended to be used in any way where its disclosure could reveal the Service's methods or sources. On the other hand, in carrying out its policing function, the RCMP has different responsibilities. In certain situations, these require it to take enforcement action the undertaking of which could oblige the Crown to disclose to the Courts information in its possession to support formal judicial proceedings. In such an event, the RCMP's information — including any obtained from the Service — is subject to legal discovery and challenge, thereby exposing the sources and the methods used in its collection to examination and public disclosure.

To prevent such an eventuality, and in properly exercising its responsibilities, CSIS places restrictions on the material and intelligence it passes to the RCMP. For example, CSIS-generated material cannot be used in formal legal proceedings without the express permission of CSIS Headquarters. This restriction has inevitably caused frustration within the RCMP, particularly among investigative personnel, who view it as a serious impediment to the efficient exercise of *their* responsibilities, and whose knowledge of the constraints on CSIS, may not be complete.

In general, we observed that at the headquarters level there were substantive efforts on all sides to understand the problems and constraints that faced both agencies. We noted a willingness on the part of CSIS

We observed cooperation initiatives being actively supported and promoted by the senior management at the headquarters of both agencies

management to accommodate the requirements of the RCMP whenever possible, particularly when the public interest in enforcement actions in a specific issue were seen to outweigh the operational and security concerns of the Service.

Some tension between the two agencies over the handling of CSIS-generated intelligence is inevitable

The Committee is aware that in certain respects, some tension between the two agencies over the handling of CSIS-generated intelligence is inevitable given the conflicting requirements. Nevertheless, incidents that came to our attention which in part gave rise to our study of the CSIS-RCMP relationship, indicate that there may be less to be sanguine about at the regional level. When we conduct our review in the regions we will be looking at the problem closely with a view to determining its seriousness and its implications for national security. The Committee will present its conclusions in the next audit report.

Potential Impact of the Supreme Court's Decision R. v. Stinchcombe

The mechanism described above by which CSIS material is protected from damaging disclosure was brought into question by the 1991 decision of the Supreme Court of Canada in the case of R v. Stinchcombe. In the view of some, the Stinchcombe decision held the potential to subject all CSIS intelligence information given to the RCMP to disclosure to the courts, regardless either of CSIS rules for its employment or whether the Crown chose to use the information in a prosecution. In such a case, any information passed by CSIS to the RCMP — oral disclosure, formal advisory letters, even meetings to discuss joint investigations — would be at risk of public exposure, thus undermining national security.

As a practical matter, however, the Committee has determined, as a result of its audit of the headquarters relationship between CSIS and the RCMP, that to date, the impact on the flow of information between the two agencies has been minimal. Nevertheless, both agencies are concerned that the current Memorandum of Understanding between them fails to reflect the realities of the situation and should be revised. The RCMP is planning to conduct an internal audit of the MOU in order to determine what changes need to be made.

The Committee is aware that a number of initiatives are being examined by various parts of Government in order to address the issues raised by R v. Stinchcombe, including possible revisions to existing legislation. The Committee intends to closely monitor this difficult issue.

Asymmetrical and Incomplete Access to Information

Another problem in the area of operational information exchange came to the Committee's attention through an earlier review conducted in the regions. CSIS places limits on access that the RCMP's liaison personnel initially have to the Service's information and intelligence. An RCMP liaison officer looking for potentially relevant information to request is only able to see material that originates in the CSIS region to which the particular RCMP liaison official is accredited; he or she does not have access to material arriving at the regional office generated elsewhere in the Service even though it may relate to matters the officer has already seen.

R. v. Stinchcombe 1991 3 S.C.R. 326.
The Stinchcombe case involved a criminal proceeding where the Crown had interviewed a witness who had given evidence earlier in the proceeding that was favorable to the accused. The Crown concluded that the evidence of this witness was undependable and decided not to call the witness in the trial. The defence sought disclosure of the interview in the belief that it might contain information favorable to its case. The Crown refused. The case went to the Supreme Court, which ruled in favour of a general duty of disclosure (other than for irrelevant information or information which was privileged) on the Crown (but not on the defence). Essentially the reasons for this ruling were:

1. Disclosure eliminates surprise at trial and thus better ensures that justice is done in a proceeding.

2. The duty of the Crown in a criminal proceeding is to lay before a trier of fact all available legal evidence: it is there to secure justice, not simply a conviction. Thus, the fruits of the Crown's investigation are the property of the public to be used to ensure that justice is done. (Defence Counsel, on the other hand, is there to defend the client's interests to the extent permitted by law.)

Stinchcombe, as such, did not deal with administrative law. The Court was careful to specify that in reaching its conclusions it was not to be taken as laying down principles for disclosure in circumstances other than criminal proceedings by indictment. For this reason, the Court did not look beyond the criminal law setting in its analysis. Notwithstanding the Court's express attempt to limit the impact of its ruling and notwithstanding the criminal nature of the proceedings, the decision has been extended to administrative proceedings. Numerous cases have emerged inspired by the principles enunciated in Stinchcombe.

In short, RCMP liaison personnel may have to make a determination about the relevance of certain intelligence material in circumstances of less than full knowledge of the existing information.

While the problem was not considered by the senior RCMP headquarters officials we interviewed as particularly serious, our earlier findings in the regions lead us to believe that there exists at least the potential for CSIS information vital to the RCMP's role and responsibilities being overlooked. The Committee believes that this issue should be examined by the headquarters of both agencies to ensure that procedural and structural factors such as these are not the cause of an intelligence failure. We intend to revisit the matter during the second segment of our study.

RCMP liaison personnel may have to make a determination about the relevance of certain intelligence material in circumstances of less than full knowledge of the existing information

Avoidable Overlap in Agency Responsibilities

The Service and the RCMP have responsibilities that sometimes involve overlapping areas of operational activity. For the most part, however, these do not present serious difficulties since the agencies have clearly defined and complementary roles set out in legislation. However, the Service has begun to devote increasing resources to an area of growing concern for all countries — the rise in transnational crime. While such an initiative may be appropriate, if not handled well and defined with precision, it has the potential of generating disagreement with the RCMP and reducing the overall efficiency of the cooperative relationship.

Cooperation between the two agencies in this area is quite recent, yet the Committee has seen early signs of disagreement. We observed that the Service's role was not fully understood by some RCMP operational personnel, who had expectations about the level of CSIS input that CSIS was not prepared to meet. In addition, we found that the terms used by CSIS to describe or circumscribe its own role and that of the RCMP in the area — words such as "strategic" and "tactical" — lacked sufficient clarity in order to be very helpful in defining areas of responsibility. For its part, the Service asserted that intelligence and law enforcement personnel do understand these concepts.

While we believe the Service may have an important role in addressing the problems of transnational crime, it is essential for a continued, productive inter-agency relationship that the role be clarified and formalized in cooperation with the RCMP. The Inspector General of CSIS has looked into the matter and the Committee intends to conduct its own study.

A Problematic Case of Inter-agency Cooperation

Report #103

In 1997, SIRC reviewed a CSIS investigation of persons in Canada who were associated with an internal armed conflict in an overseas country. During the course of the review, we identified a number of potential problems arising with respect to information the Service had provided to a Canadian law enforcement agency and a government department about a person who was the subject of CSIS investigation.

Following on allegations that the person had been involved in a foreign armed conflict, the Service commenced its investigation. While the investigation was still on-going, the law enforcement agency concerned engaged the subject to perform duties involving classified information. The person was subsequently investigated by the law enforcement agency and prosecuted for certain criminal offences.

Although the law enforcement agency had access to information CSIS had collected about the person, at first it took no action in light of the situation prevailing at the time. Later on, when the law enforcement agency learned from another source that the person was alleged to have been a party to

a foreign armed conflict, it did undertake its own investigation.

Information Disclosure Procedures

The Committee concluded that the lack of early action on the part of the law enforcement agency probably occurred for two reasons. Because of the way the system operates, the law enforcement officers located at CSIS had access to only part of the information held by the Service. The regional liaison officer did not consider the information he saw to be sufficiently noteworthy to inform his colleagues in the law enforcement agency, though, in retrospect, it was thought to be relevant to the criminal investigation. Second, the CSIS investigator concluded that the individual under investigation was not a security threat and, therefore, saw no need to pursue the matter further.

Tensions in the Inter-agency Relationship

The Committee's review of events shows that attempts to prosecute the subject caused additional difficulties between the two agencies. The police needed information from the Service to pursue the case, however, instead of following the established liaison procedures for obtaining the assistance of the Service, it employed subpoena powers to compel the attendance of CSIS officers as witnesses at the trial.

While the CSIS witnesses in the end did not testify because the charges relating to their information were dropped for other reasons, the Service believed it had cause to be concerned about the manner in which its assistance was being compelled and its information used. The recent Supreme Court ruling regarding discovery and disclosure underscores the need for proper inter-agency consultation and cooperation in the area of prosecutions involving information collected by the Service.

The second problem arose when the law enforcement agency attempted to use judicial proceedings to have the person deported from Canada. Information about the subject provided by the Service to another federal government agency with which the police was in contact appeared to have the effect of undermining the law enforcement agency's efforts. However, instead of employing any of the inter-agency consultation procedures in place, the law enforcement agency obtained a search warrant to obtain a CSIS document from a third federal government agency. To obtain the search warrant, the law enforcement agency alleged criminal wrong-doing on the part of CSIS employees. The Service states that it would have provided any information or document upon request.

The Committee believes that the Service should have provided more information about the subject to the Federal Government department concerned

The Committee's Findings

In the Committee's view, several factors led to the above events, possibly including the strong perceptions of one of the key individuals involved in the case within the law enforcement agency, as well guidance to the agency provided by the Crown Counsel involved.

First, it is evident to the Committee that when the law enforcement agency hired the person concerned, it did not subject him to the stringent Federal Government security checks required of individuals privy to sensitive information. The law enforcement

agency did not seek security screening information from CSIS and so was unaware of the allegations against the subject. While the Committee has no mandate to review the actions of the law enforcement agency, we believe there is a reasonable likelihood that none of what transpired as described above would have occurred had the Service been asked to screen the employee.

Second, the Committee believes that the Service should have provided more information about the subject to the Federal Government department concerned. A more complete assessment would have resulted in the Department being better able to address the law enforcement agency's case for deportation. The Service asserted that it would have violated the "third party rule" if it had provided more information, and that, in any event, the only important part of the letter was the Service's conclusion that the individual in question did not pose a security threat to Canada.

Third, and most important, these events underline the vital importance of sound consultative procedures between the Service and law enforcement agencies. Because of their very different mandates, the potential for misunderstanding and misperception is inherent to the work each carries out. The test of a good inter-agency relationship which serves the security needs of the country is one in which the inevitable tensions and difficulties can be dealt with quickly and constructively, on a case-by-case basis.

Areas of Special Interest — Brief Reports

When Is a Source a Source? When Is an Institution Sensitive?

Report #99

Subsequent to learning of allegations that the Service had sent a source to report on activities that could be construed as having taken place in the context of a sensitive social institution,[11] the Committee conducted a review of the matter. Our aim was to ascertain the relationship of the source to the Service, the source's activities, and whether the actions of those persons associated with CSIS complied with the laws of Canada, Ministerial Direction, and the Service's policy.

Based on our review, we concluded that no laws were broken, and that CSIS collected information on persons about whom there were reasonable grounds to suspect may have represented threats to the security of Canada. However, we did identify a potential weakness in existing policy. The relative brevity of time during which the person acted on behalf of the Service meant that a standard senior management source approval procedure was not triggered. The Committee saw this as a policy problem that ought to be addressed, and we communicated our concerns to CSIS. The Service did not agree with our assessment. Since the events described, Service policy has been changed. The time condition for management approval no longer applies.

Lawful Advocacy, Protest, Dissent and Sensitive Institutions

Sensitive operations invariably involve the use and direction of human sources, and while human sources can be the most cost-efficient form of intelligence collection, their use also entails the greatest risk in terms of impact on societal institutions, legitimate dissent, and individual privacy.

The CSIS Act specifically prohibits the Service from investigating "lawful advocacy, protest or dissent" unless carried on in conjunction with threats to the security of Canada as defined in the *Act.* The Service is obligated to weigh with care the requirement for an investigation against its possible impact on the civil liberties of persons and sensitive institutions in Canada, including trade unions, the media, religious institutions and university campuses.

In addition, the Committee attempted to determine whether the venue for the CSIS operation did in fact meet the criteria for a "sensitive institution" — a situation for which there exists specific policy direction requiring that CSIS exercise special care. While we concluded that there was insufficient information to reach such a conclusion, we also noted that the Service's definition of a sensitive social institution may be unduly restrictive. The Committee intends to pay close attention to this issue in future reviews.

A Human Source Operation

Report #102

Periodically, the Committee conducts special reviews of human source operations where there is a high risk or where a routine audit identifies an operation that we believe warrants a more in-depth examination. The case described below meets both criteria.

The two objectives of our review were to assess whether CSIS complied with the *CSIS Act*, Ministerial Direction, and its own operational policies, and to evaluate whether the risks inherent in this human source operation were justified by the information provided by this particular source.

The source was a controversial figure prior to his recruitment by CSIS. Operational policy gives senior officials the authority to approve this kind of recruitment, and the proper approvals were obtained. For the operation generally, we found that the Service adhered to the letter of Ministerial Direction and its own operational policies. For instance, when the source's activities jeopardized the integrity of the operation, CSIS suspended the relationship.

There were, however, two areas where the Committee did take issue with the handling of the source. The first concerned management practices internal to the Service. Given the potential problems that could

have arisen upon the source's suspension, we believe the Director of the Service should have been informed at the time of the decision to do so.

The second concern bore on the Service's decision to resume a relationship with the source after the initial suspension. Based on our assessment both of the source's controversial actions and the intelligence generated, the Committee was troubled by the Service's decision. The Service's comment to us in this regard was that its decision to resume contact was based primarily on his potential to provide important information in the future.

We examined the issues surrounding a serious security breach that took place within the Service several years before

Internal Security Measures

During the course of our 1997 audit, we examined the issues surrounding a serious security breach that took place within the Service several years before. When the problem first came to light, the Solicitor General directed the Inspector General of CSIS to review the matter. In the report prepared subsequently, the Inspector General stated that certain elements of the existing internal security policy were inadequate with respect to what should have been the Service's initial response to security breaches of the kind that occurred. The report also noted that policies and procedures regarding document control and site management had not been followed, and that other security practices were in need of remedial corrective efforts.

For its part, the Committee reviewed the measures subsequently taken by the Service to resolve the security weaknesses. We also examined the Inspector General's recommendations in the matter. In our view, CSIS has been fully responsive to the requirements of the situation. Document control procedures, site management, and employee internal security awareness have all been improved.

CSIS, like all federal government agencies, is obligated to comply with the Government Security Policy as set by Treasury Board. There are policies mandated by other agencies as well — for example, encryption standards are set by the Communications Security Establishment. The CSIS security policy manual elaborates on and, in some case, enhances these standards. In addition, employees of the Service are expected to know and comply with security policies; managers are responsible for their unit's performance; and CSIS human resource policies set out penalties for non-compliance with established policies, including the failure to report potential security problems.

Consequently, the Committee believes that in addition to the corrective measures already undertaken, CSIS should broadly reexamine the security policies and practices which impact on both Service responses to warnings of imminent security problems and the investigative tools available to it once they have occurred. CSIS should also consider conducting more frequent audits of employee access to its internal electronic data bases.

A Case of Historical Interest

Report #104

In the course of a previous review, the Committee located documents showing that CSIS had been in receipt of information from a foreign source about a Canadian who had allegedly spied for a hostile intelligence service in the distant past. The files also indicated that the Service had provided assistance to the RCMP in a criminal investigation of the person in question.

The Committee's interest in the matter was three-fold: to learn under what authority a CSIS employee assisted the police in what seemed clearly to be a criminal matter; to determine what the Service was seeking to gain from a case of mainly historical interest; and to review the authorizations under which Service contact with the foreign service was made.

Our review led us to understand that the foreign source was an intelligence service with which the Service had no arrangement at the time it received unsolicited information about the alleged espionage. Prior to the transfer of information, the Solicitor General had authorized the Service to establish contacts with the foreign agency concerned with a view to setting up a formal agreement. However, there is no record of Ministerial approval having been given for the Service to request a transfer of substantive information from the foreign source.

The foreign agency offered the initial information about the agent as a gesture of good faith and subsequently provided access to all of the documentation after a request from CSIS. The Service regarded the case as a means to assess the openness of the foreign agency.

The Committee's Findings

Notwithstanding the fact that CSIS obtained a targeting authorization on the alleged agent, it is the Committee's view that Ministerial permission was required prior to receiving the bulk of the "unofficial" information from foreign officials. The Service attested to the fact that the Minister was informed on several occasions about the activity and did approve of this form of liaison with the foreign agency, though the written record was silent. It is clear that the information received was vital to the unmasking of past espionage against Canada.

The Service affirmed that the information it received was unsolicited and thus did not require Ministerial approval, though it was given. We concluded that the nature of the interaction required the Solicitor General's consent.

> We strongly recommend that in all cases where the Service seeks and receives Ministerial approval, that the written record reflect that fact.

In the matter of the Service's cooperation with the RCMP's criminal investigation, our review indicates that it fully complied with the Memorandum of Understanding between CSIS and the RCMP which provides for foreign liaison assistance and support with foreign agencies on security-related matters. The files show that CSIS performed a liaison function — facilitating the RCMP's

CSIS had been in receipt of information from a foreign source about a Canadian who had allegedly spied for a hostile intelligence service in the distant past

meeting with foreign officials — and did not participate in police interviews. The Committee was satisfied that the Service cooperated with the RCMP within the parameters of operational policy, procedure, and the *CSIS Act*.

The Committee audits the entire range of CSIS investigative activities — targeting, special operations, surveillance, warrants, community interviews and sensitive operations — in a particular region of Canada

B. Annual Audit of CSIS Activities in a Region of Canada

Report #97

Every year the Committee audits the entire range of CSIS investigative activities — targeting, special operations, surveillance, warrants, community interviews and sensitive operations — in a particular region of Canada. A comprehensive examination such as this provides insight into the various types of investigative tools the Service has at its disposal, and permits the Committee to assess how new Ministerial Direction and changes in CSIS policy are implemented by the operational sections of the Service.

The Targeting of Investigations

The targeting section of the regional audit focuses on the Service's principal duty — security intelligence investigations authorized under sections 2 and 12 of the *CSIS Act*. When examining any instance in which CSIS has embarked on an investigation, the Committee has three central concerns:

- did the Service have reasonable grounds to suspect a threat to the security of Canada?
- was the level of the investigation proportionate to the seriousness and imminence of the threat?
- did the Service collect only the information that was strictly necessary to advise the government on the threat?

Committee researchers also keep watch generally on the manner of the Service's adherence to its own internal policies, rules and directives.

Methodology of the Audit

In the region at issue, the Committee randomly selected ten investigations conducted by CSIS during the 1996-97 fiscal year. However, because of changes to the Research Staff complement in the course of the review, the Committee limited the audit to seven investigations — five counter terrorism cases and two counter intelligence cases. SIRC researchers reviewed all files and operational messages in the Service's electronic data base. Researchers also interviewed the CSIS officers who carried out the investigations as well as the managers who oversaw them.

The Committee's Findings

In all cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The targeting levels were proportionate to the seriousness and imminence of the threats, and no actions were taken against non-targets. The Committee concluded that the Service, in most of the cases we reviewed, collected only the information that was strictly necessary to advise the government about the threats. Several cases, and the