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

Every year the Committee audits the entire range of CSIS investigative activities — targeting, special operations, surveillance, warrants, and the use of community interviews — 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.[16]

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*.[17] 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.

Management of Targeting

Target Approval and Review Committee (TARC)
CSIS' capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation
There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting
An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada, and are related to or emanate from that specific issue.

16. Since the 1995-96 audit of warrants was not completed in time for inclusion in the 1995-96 SIRC *Annual Report*, this audit report also presents the Committee's conclusions from last year's audit of CSIS warrant activities in a different region.

17. Section 2, paragraphs (a) to (d) define the threats to the security of Canada. Section 12 provides CSIS with the mandate for the collection, retention, analysis, and distribution of security intelligence.

Was the level of the investigation proportionate to the seriousness and imminence of the threat?

Methodology of the audit

In the region at issue, the Committee randomly selected ten investigations conducted by CSIS in the course of the 1995-96 fiscal year for study — five counter terrorism cases and five that were counter intelligence in nature. SIRC researchers reviewed all files and operational messages in the Service's electronic data base, and interviewed the CSIS officers who carried out the investigations as well as the managers who oversaw them.

Ten cases — the Committee's findings

Inappropriate targeting authority

The first case pertained to the clandestine activities of a foreign government in Canada. In the prescribed manner, Counter Intelligence Branch submitted a request to the Target Approval and Review Committee (TARC), to investigate the activities conducted or supported by a foreign state directed against Canada's economic interests. The Targeting Committee approved the Request for Targeting Authority (RTA) and the investigation began. It is the Committee's view, however, that the Service's RTA did not demonstrate a strong connection between the activities of the foreign government and potential acts of espionage against Canadian economic interests.

The Committee's analysis indicates that the RTA failed both to articulate the specifics of the economic interests it asserted were at risk or to connect the alleged activities with the particular foreign country. Appearing prominently in the request to TARC was the term "Canadian economic interests," yet the phrase was employed in a vague manner. While the targeting authorization provided the CSIS regional office with the mandate to investigate "foreign influenced activities," the examples of the activities that CSIS cited to support the request were not accompanied by evidence that these were clandestine or deceptive activities of the foreign government at issue. Nor was there an indication of a threat to any person.

The Committee has drawn the attention of CSIS officials to our conclusions on this case. CSIS asserts that sufficient and reasonable grounds existed to suspect that espionage activity had taken place in Canada.

"Issue-related" investigations

The second case pertained to an ongoing counter terrorism investigation. In January 1996, TARC renewed an earlier authorization and agreed to

Counter Intelligence and Counter Terrorism

The terms "counter terrorism" and "counter intelligence" reflect the Service's organizational structure wherein the main national security investigative functions are divided in two: the Counter Terrorism Branch addresses threats to the public safety of Canadians and national security caused by war, instability and civil strife abroad, as well as international terrorism. The Counter Intelligence Branch monitors threats to national security stemming directly from the espionage activities of other national governments' intelligence operations.

increase the intrusiveness of this particular issue-related investigation to Level 3. All CSIS regions were authorized to investigate the suspected threat of serious political violence associated with the issue.

While the Committee observed no problems with the conduct of the investigation *per se* –- regional investigators collected only the information that was "strictly necessary," and there was no evidence of extensive reporting on individuals who were not the subject of a specific targeting authority – we have serious reservations about the Targeting Committee's decision to increase the investigation's level of intrusiveness. Several CSIS regional assessments indicated that the threat was either low or non-existent, not in our view, sufficient justification to move from Level 2 to Level 3.

The Committee has also been made aware of reservations about issue-related investigations generally as expressed by the Inspector General of CSIS. In the studies supporting his 1995 Certificate, he wrote that he was concerned that issue-related investigations potentially involve entire communities and allow CSIS to collect and retain, as a part of the investigative record, a wide assortment of personal and other information on individuals and groups that are not themselves CSIS investigative targets.

The Service responded to the Inspector General stating that these "investigations were only begun when the 'reasonable grounds to suspect' standard" had been satisfied. The Inspector General was not convinced that it was possible for the grounds to be clearly documented and specific enough to justify an investigation in such cases.

The Committee shares the Inspector General's concerns that issue-related investigations can cover persons and groups who are not targets. For the case at issue, however, we found that the Service used its investigative powers with parsimony; regional investigators did not collect personal information on persons who were not subject to a specific targeting authority.

The Service used its investigative powers with parsimony

Ministerial approval for intra-government cooperation

Four of the ten audit investigations involved current or past Federal Government employees. In each case, the Committee concurs with the original decision to investigate, however, for three of the four we have concerns about the manner in which the investigation was conducted.

The Service's RTA did not demonstrate a strong connection between the activities of the foreign government and potential acts of espionage

The Role of the Inspector General of CSIS

The Inspector General of CSIS is responsible to the Solicitor General and functions effectively as the Minister's internal auditor for CSIS, reviewing the operational activities of the Service and monitoring compliance with its policies. Every year the Inspector General must submit to the Minister a "Certificate" stating "the extent to which [he or she] is satisfied," with the activities of the Service as outlined in CSIS annual report to the Minister. The Security Intelligence Review Committee also receives a copy of the Inspector General's Certificate.

CSIS has standard agreements with a number of Federal Government departments that define whether and how protected information can be released to the Service. These arrangements are authorized under section 17 of the *CSIS Act* and are approved by the Minister. In the first case at issue, the Service made several inquiries of the target's employer, a Federal Government agency with which CSIS has no such formal cooperation agreement.

CSIS investigators asked a senior official in the department to consult the person's security file and they interviewed the person's supervisor. We saw no evidence of Ministerial approval for contacts of this sort.

It is the Committee's view, however, that exchanges of information of the kind that occurred in this case constitute "cooperation" and so fall under the provisions of section 17. Furthermore, the Committee's interpretation of section 17 is that in the absence of a formal agreement, the Service still requires the Solicitor General's approval to "enter into an arrangement with or otherwise cooperate with" government agencies.

The Service still requires the Solicitor General's approval to "enter into an arrangement with or otherwise cooperate with" government agencies

> We believe that CSIS should obtain the Solicitor General's approval to exchange information with or otherwise cooperate with government departments and agencies with which it does not have formal arrangements.

Non-compliance with a formal cooperation arrangement

In another case involving Federal employees, CSIS investigators made inquiries and conducted several interviews with the target's colleagues and supervisors at his place of work. Although the Service had signed an agreement with that Federal department to share information and intelligence, the CSIS investigators sought information from employees who were not designated in the agreement. One employee did not believe that he should provide the information to CSIS. Instead, he referred the Service to another, authorized employee. The meeting that ensued was not properly documented in the Service's files.

The Service maintains that a section 17 agreement does not preclude contact with other members of a government institution, in order to collect information pursuant to the conduct of a section 12 investigation.

Reasonable expectation of privacy and the Charter of Rights and Freedoms

In the third case, CSIS acquired a certain type of information from a government agency which regarded the information as the property of the agency. The agency in question believed, therefore, that it had the authority to give the information to the Service, and CSIS officers believed no additional procedures were required to fulfill the Service's obligations under the *CSIS Act*.

Given the nature of the information and the form in which it was kept, the case raises some serious issues for the Committee. These involve, *inter alia*, the reasonable expectation of privacy on the part of the target, whether CSIS should have filed a request for the information under the

Privacy Act, and whether the manner of acquisition of the information could constitute an "unreasonable search" under section 8 of the *Canadian Charter of Rights and Freedoms*.

There is little precedent in law or in operational practice to assist the Committee to a swift finding on the matter. Following additional analysis of the information exchanged, the Committee is conducting further research into the case and its implications for CSIS policy in the future.

Allaying suspicions created by CSIS investigations

In respect of all the audited investigations of government employees, the Committee is concerned that the Service's inquiries may have left the employers concerned with a negative impression about their employees.

As a necessary part of the investigation, CSIS alerts the employers to its security concerns, but does not as a matter of course notify them about its conclusions when the investigation is complete. It is highly likely, therefore, that employers are left with the impression that employees represent continuing threats to Canada's security.

> Consequently, the Committee recommends that unless there are specific operational considerations that preclude it, the Service should in future inform Federal departments concerned about the conclusions it has drawn about Federal employees investigated.

Four cases highlighted no additional problems

In the remaining four cases, we found that the Service had reasonable grounds to suspect threats to national security. The targeting levels of the investigations were proportionate to the seriousness and imminence of the threats. The Service collected only the information that was strictly necessary to advise the government about the threats.

Obtaining and Implementing Federal Court Warrants

Obtaining Warrants - Methodology of the Audit

In order to obtain a warrant, CSIS must present its case to the Court in the form of an affidavit. Every year, the Committee examines a number of affidavits with three questions in mind:[18]

- is the affidavit factually accurate according to the CSIS information used to substantiate the affidavit;
- is the case in the affidavit presented to the Court in its proper context; and
- are the facts and the circumstances fully, fairly and objectively expressed in the affidavit.

In order to satisfy ourselves that the affidavits are appropriate, we compare the facts presented to the information found in the Service's files.

Committee findings, 1994-95 warrant affidavits

Incomplete affidavits

Two affidavits were examined. The first was an emergency request from

The Service's inquiries may have left the employers concerned with a negative impression about their employees

18. Over the course of the last fiscal year, the Committee completed reviews of Federal Court warrants obtained by CSIS in two regions. The first review began late in 1995-96 for the period 1994-95 and we were unable to present our conclusions in that year's annual report. The second warrant review took place in 1996-97, for activities in 1995-96, and covers the same region as the other audits in this chapter.

the regional office, and while we found the urgency of the warrant to have been justified, we believe the affidavit could have been prepared with greater care. For one of the persons targeted by the warrant, the affidavit overstated a fact. For another person targeted, the Service failed to include in the affidavit significant information of which it was aware which contradicted its own position on the person.

The second application sought a renewal of warrant powers against a long-standing CSIS target. The Committee noted a minor contradiction between the affidavit and the information in the Service's files. Had this contradictory information been included in the affidavit, the Court would have been more fully informed of all the relevant facts. In general, however, the affidavit was factually accurate and correctly defined the context of the investigation.

Inaccurate tracking of warrant preparation

The procedures by which CSIS tracks the preparation of warrant applications is also of interest to the Committee. Normally, warrant applications are reviewed both within CSIS and the Ministry of the Solicitor General to ensure that the affidavits are operationally and legally correct. An independent legal counsel from the Department of Justice then serves as an objective final assessor of the affidavit and the facts supporting it, prior to submission to the Federal Court.

The preparation process is tracked in diary form, which in the case of one affidavit, seemed to indicate to the Committee that the independent legal counsel did not have sufficient time to review the extensive documentation supporting the application. The Service subsequently informed the Committee that while it was not recorded in the tracking system, the independent counsel had in fact received a time extension to allow him to conduct a proper review before the warrant was obtained.

Committee findings, 1995-96 warrant affidavits

Again the Committee examined two affidavits and supporting documents in depth. For one warrant, in the counter intelligence area, we found no errors or omissions, and no problems of balance in the presentation.

The Use of Warrants to Investigate Threats to National Security

If during a CSIS investigation a section 21 warrant is required to investigate threats to national security, the Service must seek approval from the Federal Court. CSIS Legal Counsel, with the assistance of Service analysts, prepares an affidavit in support of the warrant to present to the Court. The affidavit explains why warrant powers, such as telephone intercepts, are needed, and the document must also meet other statutory requirements. For example, under section 21(2)(b) of the *CSIS Act*, the Service must show that other investigative means have failed, or are "unlikely to succeed." The warrant granted on the basis of the affidavit lists the powers given to CSIS, who will be subject to them, and where they may be deployed. The warrants also contain any conditions imposed by the Court on the manner in which CSIS can carry out its investigation.

Discrepancies in an affidavit

However, with the second audited warrant — directed at counter terrorism targets — we found a number of discrepancies between the statements in the affidavit, and the documents in the "schedule of facts." In several cases, the Service wrote that it had "established" certain associations or certain patterns of contact. The supporting documentation, however, was often equivocal, and in our view, the facts appeared to be weaker than the language suggested. In some cases, the schedule of facts contained documents that seemed to contradict the Service's case.

In the view of the Committee, these discrepancies did not undermine the case for targeting the persons named in the affidavit; that is, the affidavit was fundamentally sound, and the security threat it addressed was serious. Most of the problems stemmed from documents that were omitted from the schedule of facts, and the discrepancies between the supporting documents and the affidavit.

After conducting further research, we concluded that this particular affidavit was an aberration, and not a trend. We believe, however, that CSIS should maintain a consistent high level of rigour in the process of compiling and reviewing facts and supporting documentation, employed in affidavits.

Warrant implementation – findings

The Committee reviewed the implementation of warrants against two CSIS targets and found the Service to have complied conscientiously with the warrants' terms and conditions.

Warrants for two new areas of inquiry

An additional focus of this year's review of warrant implementation was an examination of the new challenges the Service faces in exercising powers granted by warrants. Federal Court warrants are now required for two new areas of inquiry, which have "reasonable expectation of privacy" implications which the Service has recognized.

The Committee has recommended that CSIS adopt clear policy about the requirement for a Federal Court warrant to collect information in these instances.

As this is a new area, the Committee intends at a later date to conduct an in-depth review of the impact on the Service's requests for and execution of these warrants.

We believe the affidavit could have been prepared with greater care

Audit of Sensitive Operations and Associated Ministerial Direction

Methodology of the audit

The very nature of sensitive operations dictates that they are the subject of relatively frequent Ministerial Direction. In addition, policy for implementing sensitive operations is set out in some detail in the *CSIS Operational Policy Manual* and all requests for sensitive operations, depending on the level of sensitivity, require at a minimum, the approval of Service senior management.

"Reasonable Expectation of Privacy" and Canadian Law

The phrase "reasonable expectation of privacy" encapsulates a vital principle of Canadian law with respect to when and under what conditions the State may intrude on the privacy of an individual. Managing security intelligence involves constant weighing of the balance between two imperatives — individual privacy and threats to Canada. In commenting for the Department of Justice on the Supreme Court of Canada's *Charter of Human Rights and Freedoms* decisions in this area, Graham Garton, Q.C. wrote:

> Respect for individual privacy is an essential component of what it means to be "free." As a corollary, the infringement of this right undeniably impinges upon an individual's "liberty" in our free and democratic society. It is apparent, however, that privacy can never be absolute. It must be balanced against legitimate societal needs. This Court has recognized that the essence of such a balancing process lies in assessing reasonable expectation of privacy and balancing that expectation against the necessity of interference from the State. Evidently, the greater the reasonable expectation of privacy and the more significant the deleterious effects flowing from its breach, the more compelling must be the State objective, and the salutary effects of that objective, in order to justify interference with this right: R. v. O'Connor, [1995], 4 S.C.R. 411.[19]

For the purposes of the audit, the Committee examined a set of randomly selected human source investigations. In addition, we reviewed all requests from the Service for Ministerial approval of and all requests to CSIS senior managers pertaining to operations involving "sensitive institutions" or any operations dealing with lawful advocacy, protest and dissent.

Committee findings

No attempt to influence sensitive institutions

In none of the operations involving sensitive institutions that we examined did CSIS attempt to influence or direct the activities of the organizations, and source management in this regard was in compliance with the most recent Ministerial Direction.[20] In most of the cases, the sources' associations with the respective organizations were not at the behest of the Service.

Ambiguity in source direction

In one of the selected cases, the Committee found the Service's officers seemed to be unnecessarily indecisive about whether to advise a source to report a crime the person had information about to the authorities. The source thus received an ambiguous message concerning the commission of criminal acts by others. The Committee believes that the Service should have clearly counselled the source to report the information to the appropriate authorities.

Senior management approvals for operations

Of note among the senior management approvals for operations the Committee examined were the following:

The Service approved a request for a source to participate in a demonstration that had the potential to

19. Department of Justice, March 1997.

20. The management of human sources, their participation in an organization's activities and the impact of new Ministerial Direction is examined by the Committee in detail at page 10 of this report.

become violent. The source had little choice but to participate and the Service appropriately counselled him on how to avoid violent incidents.

Three approvals granted dealt with operations involving academic institutions; one of these raised a substantive issue.

Under Ministerial Direction — since revised— any use of a source on campus had to be approved by the Solicitor General. Under the procedure which obtained at the time, the Minister approved the use of a source on a particular campus.

The Service subsequently directed a second source to attend the same event under the initial approval. It is the Committee's view that the Service's action in this context was a clear contravention of the spirit of the 1984 Ministerial Direction[21] on university campus investigations.

Retention of sensitive information on non-targets

Section 12 of the *CSIS Act* stipulates that information can be retained by CSIS in regard to threats to the security of Canada only to the extent that it is "strictly necessary." The Committee found during its examination of one of the audit cases that the Service was holding information in a computerized data base that clearly did not fall into this category. The report at issue contained personal and sensitive information about a person who had never been a CSIS target nor the subject of an investigation, but instead had been interviewed as a potential source.

> The Committee recommends that source recruitment assessments involving persons who are not targets not be retained as part of the Service's section 12 data base.

The Service informed us that it has taken corrective action.

The Surveillance of Groups and Persons

The Committee reviewed a sample of targets who were the subject of

In none of the operations involving sensitive institutions that we examined did CSIS attempt to influence or direct the activities of the organizations

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.

21. See "Ministerial Direction" page 52.

surveillance coverage in fiscal year 1995-96. We examined the surveillance reports to determine whether the surveillance,

- conformed to the requirements and restrictions set out by the Target Approval and Review Committee (TARC);
- exceeded the "strictly necessary" provision of the *CSIS Act*, or otherwise unduly or unnecessarily infringed on a person's privacy; and
- complied with Ministerial Direction and the *CSIS Operational Policy Manual*.

. . . the Committee was satisfied to see that CSIS regional employees made considerable efforts to understand the homelands conflicts. . .

Committee findings

Our review of selected cases indicates that the Service complied with all policies and procedures for carrying out surveillance operations and conducted them in an appropriate manner. There were no occasions where emergency requests for surveillance were made in the Region we audited.

Quality of surveillance with reduced resources

Surveillance is a resource-intensive activity. In the region we reviewed, the Committee did not find that the selective tasking for surveillance and the Service's diminishing resources had a negative effect on the quality of surveillance operations.

Interviews Within Particular Communities

Since 1990, CSIS has employed community interviews regularly in order to learn more about potential threats to Canada's security from the spillover of overseas "homelands" conflicts into Canada. The interviews also serve to sensitize ethnic communities about the aims of the Service and its role in protecting the security of Canada and Canadians. In the region the Committee audited for this report, three programs to interview leaders of communities or interest groups were underway.

As in past audits of community interviews, the Committee's concern was to determine whether the interviews were conducted in a proper manner. Specifically, were they properly authorized; was the information collected and retained only that which was "strictly necessary"; and was the scope of the interview program appropriately defined.

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.

In general, the Committee was satisfied to see that CSIS regional employees made considerable efforts to understand the homelands conflicts figuring prominently in the current interview programs. As part of the preparatory work, the investigators reviewed background reports from other Government of Canada departments.

Findings of the Committee

Interview program I

The Service considers this community interview program to have been the most successful and the Committee concurs. To date, neither CSIS nor SIRC have received a single complaint relating to the interviews conducted.

The Committee saw no evidence that the Service collected inappropriate personal information about those persons interviewed. It retained only what was "strictly necessary" to advise the government. Investigators asked questions regarding the potential for violence or foreign influence in the ethnic community and the impact of Canada's military role in the conflict.

The Service's Regional office noted that there had been isolated incidents of inter-ethnic community harassment by what it termed "hot heads" during the period under review, but stressed that there was no trend to widespread or serious violence. With regards to foreign embassy interference, the Service observed none of consequence.

The Committee believes that as the overseas conflict winds down, we would expect to see the end of this particular community interview program.

Interview program II

The second community interview program revealed an apolitical community which, while concerned about the unfolding events overseas, did not manifest a potential for violence in Canada. The Regional office noted that during the period of the interviews, a foreign mission in Canada tried to apply subtle influence on the community to refrain from political involvement in the home country.

The Committee noted that CSIS interviewed relatively few people and that the investigators appeared to be respectful of those they spoke to; we saw no evidence of the collection of inappropriate information.

The interview program was terminated after six months — a decision the Committee believes was valid considering the paucity of reasonable grounds to suspect a threat to national security arising from the ethnic community in Canada.

Interview program III

The Committee identified no difficulties with the few interviews conducted in this program, but did take issue with the fact that the investigation was set in motion in the first instance.

The targeting authorization referred to information from foreign services to the effect that overseas extremists might have taken root in Canada. This prompted CSIS to develop the community interview program. The

The Committee saw no evidence that the Service collected inappropriate personal information about those persons interviewed

The Committee did take issue with the fact that the investigation was set in motion in the first instance.

Committee saw no evidence in the documents to sustain that premise.

The Service has acknowledged that while it was unaware of any extremists or their supporters in Canada at the time, threats of violence from extremists overseas remained a concern, as did a potential indirect threat to Canadians living overseas. The Committee noted, however, that the content of interviews focused on what was happening in Canada, not on the events taking place abroad.

In any event, the investigation failed to corroborate the original information or to identify possible affiliates of extremist organizations in Canada. The Service subsequently elected to allow the investigation to conclude upon the expiry of the targeting authority and stated that it would monitor any future developments related to the threat via its other investigations.

Development of written policies for community interviews

The Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program

The Committee is pleased to note that the Service acted on a previous SIRC recommendation and elaborated a policy which would compel investigators to inform interviewees that their cooperation is voluntary.

As in previous years, the Committee remains concerned about the ambiguity evident in the definition of what constitutes a community interview program. The correspondence that CSIS sent us to explain the issue was helpful, and we believe the Service should consider adding the information to its policy.

> The Committee recommends that the definition of community interview programs be clearly set out in CSIS policy.

In a related policy matter which remains unresolved, the Committee recommended in its last audit that the Service update its *Operational Policy Manual* to include an existing memorandum on procedures for community interviews. We have seen no corporate policy revisions in this area to date.

C. Inside CSIS

The third part of this section dealing directly with what CSIS does and how it does it, consists of the Committee's comments and findings on how the Service manages its own affairs and its relations with other agencies of Government and other national governments.

Statistics on Operational Activities

By law, the Committee is obliged to compile and analyse statistics on the operational activities of the Service.

Annually, the Service provides the Committee with statistics in a number of areas: warrants, sensitive operations, finances, person-year usage and the like. We compare them against the data from previous years and question CSIS about any anomalies or new trends that we identify.