



SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Report 1999–2000

An Operational Audit of the
Canadian Security Intelligence Service



**SECURITY INTELLIGENCE
REVIEW COMMITTEE**

SIRC Report 1999–2000

**An Operational Audit of the
Canadian Security Intelligence Service**

Canada

Security Intelligence Review Committee
122 Bank Street
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

Tel: (613) 990-8441

Fax: (613) 990-5230

Web Site: <http://www.sirc-csars.gc.ca>

Collect calls are accepted, and the switchboard is open
from 8:00 a.m. to 5:30 p.m. Eastern Standard Time.

© Minister of Supply and Services Canada 2000

Cat. No. JS71-1/2000

ISBN 0-662-65238-X

The Honourable Lawrence MacAulay, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

30 September 2000

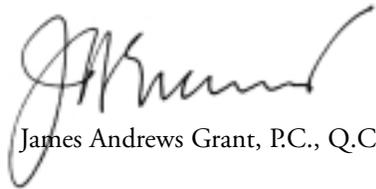
Dear Mr. MacAulay:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 1999–2000, for your submission to Parliament.

Yours sincerely,



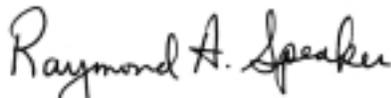
Paule Gauthier, P.C., O.C., Q.C.
Chair



James Andrews Grant, P.C., Q.C.



Robert Keith Rae, P.C., Q.C.



Raymond Speaker, P.C.



Frank McKenna, P.C.

Statement from the Committee

From the community of people who pay special attention to security intelligence matters—be they journalists, academics, parliamentarians, lawyers or intelligence professionals—we hear many views of what the Security Intelligence Review Committee should be doing and how. We know this because we make special efforts to solicit those views and create opportunities for them to be expressed, and because the interest of the media in security intelligence issues has rarely been greater than in the past year.

Not unexpectedly, the messages we receive are diverse and often contradict each other: “You take too much time”; “Your studies are not as extensive as they should be”; “You aren’t tough enough on CSIS”; “Your review process interferes with the vital business of ferreting out threats to the country.” From amongst these conflicting judgements about our work and how it relates to the task of the Service, one clear theme emerges. We continue to hear concerns about whether the system that governs the country’s security intelligence apparatus is adequately protecting individual rights.

The Committee has been made acutely aware of these concerns over the past year because of the outcome of three complaints about immigration security screening on which we rendered decisions. Despite our findings

that showed clearly that the Service had erred in the procedures used to conduct its investigations and in the advice it had given to the immigration authorities, three people continue to wait for their immigration status to be resolved.

Because the Committee’s mandate gives us the ability only to advise the Government on these matters, we can neither make directives nor change policies. Consequently, if the relevant government authorities fail to redress the wrongs our own investigations have identified, dissatisfaction with, and cynicism about, Canada’s system for dealing with immigration security screening matters can be expected only to grow—at the very least on the part of these three complainants and their legal counsel.

The Dilemma of Security Intelligence

More generally, the Committee understands that the public’s doubts about security intelligence have quite rational origins. One is the way in which security intelligence work in any democracy takes place, wherein the government gives a small group of people powerful and intrusive investigative powers and instructs them to tell almost nobody about what they are doing. The natural instinct of an aware citizenry is to wonder what on earth those people might be up to.

Another reason is grounded more specifically in the Canadian experience. Only two decades ago, the McDonald Commission laid out in painstaking detail the ways in which CSIS' organizational predecessor, the RCMP Security Service, was essentially out of control.

A third reason for concern stems from the profound social and economic changes wrought by technology and globalization. More than ever, Canadians inhabit a world of strongly competing loyalties—national, ethnic, religious and political—and although Canada is and should be open to all different kinds of people, Canadians are also aware that conflicts between these loyalties can sometimes take a violent form.

That Canada needs CSIS and the work it does, in the Committee's opinion, is not in doubt. But the mere existence of CSIS creates a dilemma for Canadian democracy: democratic government requires that its activities be as transparent as possible and that its institutions be accountable. At the same time, the essence of democracy is to balance conflicting interests in ways that best meet the collective interest—itself not always readily defined—of all citizens. Protecting that democracy and its citizens from serious threats sometimes calls for intrusive methods and requires that certain information about these activities be withheld from general knowledge. The resulting absence of hard facts leaves an information vacuum ready to be filled by speculation, suspicion and conspiracy theory.

An Elusive Balance

Although the legislation creating SIRC states that it is to “review” the activities of CSIS and report to Parliament, the Committee also sees its role as one of helping to address the challenges and dilemmas raised by the need to carry out security intelligence work out of public view. In all our activities, we strive to balance the need to protect individual rights with the state's obligation to protect against threats to Canada and Canadians.

One of the tools given to the Committee in grappling with these difficult, sometimes intractable issues was that of professional and independent inquiry. Specifically, the legislation states that the Committee is to have access “to any information under the control of the Service” relevant to the performance of its review duties. In short, we look at everything the Service does; we ask questions and then we ask more questions. We poke and prod and read and dig. As one might expect, CSIS sometimes gets impatient with us and is often displeased with our conclusions, but that is the Committee's job, which no other body in Canada is equipped to do.

It was in the context of our special mandate that, during the past year, we commented on a revised immigration law currently before Parliament. Bill C-31 would, among other measures, transfer from SIRC to the Federal Court a particular appeal process available to prospective immigrants about whom adverse information has been collected by the Service. In a report sent to the Solicitor General (under section 54 of the *CSIS Act*) about the new legislation, the Committee drew attention to SIRC's unique expertise in acting as the competent tribunal to handle appeals related to security intelligence and security screening matters—a capacity Parliament intended the Committee to have and which it has given to no other body. We believe that this proposal would remove important existing safeguards on the activities of CSIS that could have a serious negative impact on national security, on individual rights, or on both.

Reporting in the Public Interest

Another important function Parliament gave to SIRC was to report publicly. In this matter the legislation is less specific—the Committee must report to Parliament (and thus to the people of Canada) once a year about its activities. However, nothing is said about the nature of the reporting or how detailed it should be.

There are some who would prefer the Committee adopt a minimalist approach to its reporting tasks. Our job, they contend, is to assure Parliament that the Service is acting within the law and to leave it at that. However, from the beginning in 1984 and continuing to the present, Members of the Committee have adopted the view that more is better. Although our own reporting to Parliament and the people of Canada still suffers occasionally from the obfuscation made necessary by security concerns, the Committee has consistently pushed to deliver as much information as possible to the public. The Committee has fought and won countless small battles over whether a particular disclosure was damaging to national security or merely unsettling to the Service.

The main reason for the Committee's assertive approach to reporting is that we are mindful of the unique powers vested in us. The law and simple prudence about sensitive security matters dictate that the vast majority of citizens must trust in us to make sure that CSIS functions responsibly. As we have stated on other occasions, this trust must be earned and constantly nurtured.

The report that follows fulfills our legal obligation to Parliament, and we are ready and eager to discuss these and other matters with Parliamentarians. The report also reflects the Committee's continuous efforts to inform the public about security intelligence issues and draws together a year's work reviewing all facets of the Service's activities. Every study conducted, every query pursued, every complaint acted upon is reflected in its pages.

We hope that, in giving credit to CSIS when it is deserved, and pointing out shortcomings—and remedies—when and where we find them, the Committee can help replace speculation with fact and suspicion with trust.

How SIRC's Annual Audit Report is Organized

The report is organized to reflect the Committee's primary functions: first, to review CSIS intelligence activities, second, to investigate complaints about CSIS and associated matters, and third, to act in concert with other parts of the governance system to protect Canadians from threats to their security.

- Section 1 presents the Committee's review and audit of what the Service does and how it does it. The subsections represent the different methods the Committee employs to make these assessments.
- Section 2 deals with the Committee's role as a quasi-judicial tribunal with the power to investigate complaints of various kinds.
- Section 3 brings together under one heading—CSIS Accountability Structure—the Committee's review of the multiple administrative and legal mechanisms that hold the Service accountable to Government, Parliament, and the people of Canada.

As before, the report draws a clear distinction between Committee comments, observations and recommendations bearing directly on our major task—reviewing CSIS and associated activities for a certain period—and the more general background material we are making available with the aim of assisting Canadians and other readers to understand the context in which security and intelligence work is carried on.

Subjects the Committee believes will be of historical, background or technical interest to readers are set apart from the main text in shaded insets. Unlike the main body of the report, they do not reflect Committee opinion or conclusions as such and are intended to be factual in nature.

Each section of the audit report is labelled with the SIRC study from which it is abstracted. The full references are found in Appendix B.

A. Areas of Special Interest for 1999–2000

Project Sidewinder

Report #125

BACKGROUND TO THE COMMITTEE'S REVIEW

In September and October 1999 a series of newspaper articles appeared about a RCMP–CSIS project with the codename “Sidewinder.” According to the reports, Sidewinder was a “top secret government project” launched in 1995 and staffed by a joint team of “civilian and police analysts and investigators” from both CSIS and the RCMP. The overarching theme of the media reports was that the project had been the subject of improper political interference damaging to the national interest.¹

The principal assertions in the media were:

- that the goal of Sidewinder was to gather and analyze intelligence about efforts by the Chinese Government and Asian criminal gangs to influence Canadian business and politics;
- that the Project was terminated before completion because the Service anticipated political resistance;
- that CSIS improperly destroyed all copies of Sidewinder’s final report, as well as drafts, correspondence and other related documents;
- that ending the joint project in 1997 was premature and subsequently hobbled the government’s ability to deal with emerging threats to the country;
- that the Sidewinder team’s request for additional resources, and its recommendation to CSIS/RCMP management to launch a formal investigation into

the alleged activities were answered by the project being terminated and the team being disbanded;

- that the mismanagement of Project Sidewinder had significantly harmed overall relations between CSIS and the RCMP.

SCOPE AND METHODOLOGY OF THE AUDIT

The Committee’s review of Project Sidewinder encompassed all available documentation created or collected by CSIS since the project’s inception; interviews with Service and RCMP officers involved in preparing Sidewinder reports; correspondence with and interviews of outside parties offering information or documentation to the Committee; and an examination of all relevant documents in the Service’s files.

In view of the Committee’s mandate to review the activities of CSIS, our efforts were necessarily focused on the Service’s actions. Nevertheless, the Committee did gain access to some, though not all, Sidewinder-relevant files held by the RCMP, specifically those relating to project administration and report drafting. In addition, we were able to interview RCMP officials.

Of all the Sidewinder documents reviewed, the lion’s share originated from RCMP and not from Service files. In the period following the completion of the first draft report in 1997, the Service had disposed of most of the Sidewinder documentation in its possession. In response to a query from the Committee, the Service said that its action was appropriate and fully in accordance with standing CSIS practice for the disposal of files. This matter is discussed more fully below.

THE GENESIS OF SIDEWINDER

Only the second joint project of intelligence analysis ever undertaken by CSIS and the RCMP, the organizations signed a “Joint Analytical Plan” for Sidewinder in March 1996. Making use of public, open-source information, and data already at hand in CSIS and

Main Points

- The Committee found no evidence of political interference as alleged. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.
 - With respect to the Sidewinder first draft report, we found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.
 - The Committee found no evidence of any substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.
 - The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused, or were symptomatic of, difficulties in other areas of the inter-agency relationship.
 - The Service disposed of what it regarded as “transitory documents” related to the Sidewinder first draft report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather “misfiled.” However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.
-

RCMP files and those of co-operating agencies, the project was to assess the threat to Canadian security from certain foreign interests. Four people were assigned to work on the project; two analysts from each agency. During the course of the project, expected to take several months, the team would produce interim “intelligence briefs” updating the Government and allied agency clients on national and international links, and intelligence trends disclosed during the analytical process.

The final report would include link diagrams, flow charts and personal profiles. The Sidewinder team would also prepare, “as required,” a multi-media

presentation highlighting threats to Canada identified as a result of the project. According to the plan, the principal, or at least initial, clients for the project were to be RCMP and CSIS management, with the Service side of the project being managed by the Requirements, Analysis & Production Branch (RAP). RAP products are typically disseminated to a wider readership within government and, where appropriate, the intelligence services of allied countries. One can assume, therefore, that at least on the CSIS side, products of Sidewinder research were expected to reach a wider readership.

Sidewinder team members began by developing a “collection plan”—which data to collect and how.

Under the plan, information of interest was to be identified by cross-referencing information in RCMP and CSIS computer databases. Team analysts would make use of existing CSIS and RCMP files, and the assistance of two other government departments would be solicited to supplement the information base. Records checks would be run through departmental databases, and domestic law enforcement agencies with expertise in the area would also be consulted.

THE ILL-FATED FIRST DRAFT

According to the plan, the project was to complete its analysis by mid-November 1996. However, the available records appear to bear out what the Service told the Committee, that, irrespective of the plan, “little action was taken beyond the production of an initial draft which proved to be unacceptable.” Even in this, there was a delay of some six months.

The RCMP told the Committee that the frequent turnover of CSIS personnel dedicated to the project contributed to the delay. For its part, the Service told us that the staffing changes were the result of internal reorganization, transfers and retirements, all unrelated to Sidewinder itself.

The first draft, completed in May 1997, arrived at two key conclusions: that the potential threats warranted the deployment of additional government resources, and that the authorities (RCMP/CSIS) should take the steps necessary to alert operational managers in the RCMP and CSIS to the need to investigate further.

According to the RCMP, the two agencies were scheduled to examine the paper in a “joint review board” on June 9, 1997. Prior to the joint board, however, the Service convened its own internal review, and then shelved the report because, according to the Director General RAP, its findings were “based on innuendo, and unsupported by facts.” The RCMP objected to the circumvention of the joint board review procedure and encouraged the analyst/authors

of the first draft to prepare a facting binder in support of the report’s assertions. Work on Project Sidewinder was suspended, while discussions between the Service and the RCMP about its future continued.

SIDEWINDER RESUMES, DIFFERENCES EMERGE

In January 1998, CSIS and the RCMP agreed to resume work on Project Sidewinder and the production of what would become the final report. The only change made in team staffing was to replace the senior Service analyst, which CSIS attributed to the internal RAP branch reorganization. The new CSIS analyst became the principal author of Project Sidewinder’s final report, completed a year later.

Having resumed work, the Sidewinder team began producing new report drafts for Service and RCMP managers to consider. Disagreements between the two agencies soon arose. In May 1998, the RCMP Chief Superintendent in charge of the Force’s side of the Project wrote to his equivalent at the Service (Director General RAP) about a number of factual errors he saw in the revised draft. He took issue with the draft’s “Conclusion” and “Outlook” sections and asked that they be rewritten. It is apparent from the correspondence that the revised draft had taken a noticeably different tack from that of the contentious first draft.

In September 1998, a CSIS Sidewinder analyst wrote to his RCMP counterpart in the Criminal Analysis Branch requesting additional supporting information. The RCMP’s Officer in Charge (OIC) responded to the request by writing to CSIS (Director General RAP) that the RCMP would provide no further information: “It is our opinion that we have provided sufficient background information in support of the materials provided by the RCMP.”

In December 1998, the Deputy Director General RAP wrote the RCMP OIC pointing to innuendo in

the then-current report draft and asking that it be removed. She wrote: “We do not have factual evidence of our suspicions and the Service is uncomfortable with the obvious challenges that could be raised by the readership.” She added that in her view both agencies had to concur with the inclusion of items in the joint paper, and “regrettably we [CSIS] cannot in this case.”

SIDEWINDER FINAL REPORT

In January 1999, the Sidewinder final report was completed, which both agencies approved for distribution. CSIS informed us that the RCMP officially accepted the revised report and a copy of it bears the note “Good Report” penned by the responsible RCMP Chief Superintendent. In response to Committee queries, however, that official wrote that the Force

Government, Parliament and the people of Canada were properly served by the advice they received from the agency responsible for assessing threats to Canada and Canadians.

FINDINGS OF THE COMMITTEE

Was There Political Interference?

A media report early in the public discussion of Sidewinder asserted that the project was shut down in mid-stream because CSIS anticipated political resistance. Immediately obvious to the Committee was that the first claim, that Sidewinder was terminated, was simply wrong. Work on Project Sidewinder was suspended temporarily in June 1997 and restarted in early 1998.

The Committee could find no evidence of political interference as alleged. None of the documents or records we reviewed or received evidenced such interference, actual or potential. None of the CSIS and RCMP employees we interviewed had knowledge of political interference or interference by other agencies in Sidewinder or in other related investigations. None of the other parties who came forward to contribute to our review had knowledge of interference or offered substantiating information of any kind.

Was the Service Right to Shelve the First Draft Report?

The Committee studied the first draft report and found it to be deeply flawed and unpersuasive in almost all respects. Whole sections employ leaps of logic and non-sequiturs to the point of incoherence; the paper is rich with the language of scare-mongering and conspiracy theory. Exemplifying the report’s general lack of rigour are gross syntactical, grammatical and spelling errors too numerous to count.

It is apparent to the Committee that, at its core, the Sidewinder first draft lacked essential definitional

With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence

was “not fully satisfied with the final report” because unlike the first draft it “fails to raise key strategic questions and to outline some of the more interesting avenues for research.”

The Committee has read both Sidewinder versions and the differences between the two are considerable—the quality and depth of analysis in the final version is far higher than in the draft. Clearly a great deal went on between completing the first draft and releasing the final report many months later.

The essential issues for the Committee, therefore, were whether the Service’s actions were appropriate during this time, in line with policy and Ministerial Direction and within the law; and whether the

clarity: if one purports to examine the extent of illegal and threat-based activities allegedly taking place alongside entirely legal and benign ones, it is vital to be able to tell the difference between the two. Sidewinder's first draft drew no such distinctions, providing instead a loose, disordered compendium of "facts" connected by insinuations and unfounded assertions.

The Committee believes that the Service correctly assessed the first draft and took appropriate actions to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality. The Committee believes further that both actions were consistent with the Service's responsibility to assess threats to Canada and Canadians rigorously and in a professional manner and provide objective advice to Government based on those assessments. As it stood in May 1997, Project Sidewinder's first draft report failed to meet those standards.

Did Sidewinder Harm the CSIS–RCMP Co-operative Relationship?

That the CSIS–RCMP relationship continues to be productive and fruitful is vital to the safety and security of Canadians, and monitoring the quality of the Service's co-operative arrangements with the RCMP is of on-going concern to the Committee.² Although the Committee's review of Project Sidewinder revealed significant differences of opinion and institutional perspective between the Service and the RCMP over the project, we saw no evidence that the difficulties encountered here were symptomatic of a more widespread problem. Nevertheless, the Committee did attempt to identify the sources of friction and obtain each agency's views of the most significant problems.

The difficulties began after the joint analytic team completed the Sidewinder first draft report. Simply put, RCMP management believed the first draft was good work that went some way to proving the initial thesis, whereas the management of CSIS thought the report's findings were based on innuendo and were

not supported by the facts. The Service insisted on a radical rewrite.

CSIS managers told the Committee that among other things, difficulties arose from the inability of the team of analysts to take criticism well, from the fact that the report offered broad recommendations for action when RAP reports typically stopped at analysis and because the report's recommendations were an attempt by some in the RCMP to obtain more resources.

The RCMP's diagnosis was quite different. In interviews and correspondence with the Committee, RCMP management responsible for the project expressed frustration with the Service's approach to the approval mechanism for the joint report which both organizations had agreed to at the outset of Sidewinder. They said that their own analytical reports often came with recommendations and that it was evident that a difference of opinion existed on what constituted good strategic analysis. Finally, the RCMP expressed the view that Service management seemed prepared to ignore the results of a full and impartial joint review.

As noted above, the Committee believes that Project Sidewinder has inflicted no lasting damage to the broader CSIS–RCMP relationship.

Did Shelving Sidewinder's First Draft Imperil Canada's National Security?

Some media reports about Sidewinder in late 1999 portrayed the rejection of the Sidewinder first draft report and its subsequent revision as having blinded the Government to certain emerging threats, such as the abuse of the immigration process. The Committee found no evidence of any kind that such was the case.

Although the delivery of the Sidewinder final report effectively marked an end to the joint effort, both CSIS and the RCMP have continued, separately, to explore and analyze the potential threats to Canada.

Is There a Substantial Threat to Canada That Has Been Ignored?

The *CSIS Act* sets out the threats to national security the Service is responsible for looking into. Measured against these definitions, the Committee's review revealed no "smoking guns," no evidence of substantial and immediate threat, and no evidence that a threat was being ignored through negligence or design.

Did CSIS dispose of documents improperly?

At the outset of our review, the Committee was informed that CSIS had disposed of almost all documents³ related to producing the first draft of the Sidewinder report (documents pertaining to the final report had been retained and were reviewed.)⁴ The question for the Committee was whether these actions were appropriate and carried out in accordance with policy and law.

The Service's document control procedures lack rigour and its reviews have not been as effective as the Service and we would have wished

In response to Committee inquiries, the Service stated that the disposal of working documents was standard practice for all analytical reports prepared by RAP (the anchor for the CSIS end of the joint project) and was fully in accordance with Government policy. The essence of the Service's case was that the documents disposed of fell into the category of "temporary or transitory records," used in preparing an analytical collaboration, and as such were not retained beyond their need in accordance with National Archives of Canada policy.

Subsequently, however, the Committee determined that some documents the Service was not able to provide to the Committee were not transitory in nature—specifically, inter-agency correspondence concerning the drafts, as well as the signed agreement between the RCMP and the Service setting out terms of reference for the original joint Project.⁵

When the Committee made the National Archivist aware of these particulars, he wrote to us that the Service had already responded satisfactorily to his own inquiries. When we brought the matter to the attention of the Service, it stated that those particular missing documents had not been disposed of like the others, rather they had been "misfiled" and so could not be located.

Because almost none of the Sidewinder first draft documents were to be found at the Service, the Committee is not in a position to render a judgement on the appropriateness of the original disposal. Some were legitimately disposed of and the balance were lost—but we are unable to determine with any certainty which was which.

The Committee finds the evident confusion over the documents' whereabouts disconcerting. The essential trade of security intelligence is meticulous document control and information management. We reiterate our comments made in the "Lost Documents" study (*see* page 9) that the Service's document control procedures lack rigour and its reviews of its practices in this area have not been as effective as the Service and we would have wished.

Notwithstanding our concerns over the Service's handling of some of the Sidewinder documents, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder. In any case, the Committee found no evidence that raw information, kept in Service files and used by the

Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

MAIN POINTS AND CONCLUSIONS

With respect to allegations of political interference in the course of Project Sidewinder, the Committee could find no evidence. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.

With respect to the Sidewinder first draft report, the Committee found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.

The Committee found no evidence of substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design, and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.

The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused difficulties in other parts of the inter-agency relationship.

The Service disposed of what it regarded as “transitory documents” related to the first draft Sidewinder report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather “mis-

filed.” However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

In conclusion, the Committee considers the vital lesson of Project Sidewinder to be this: It is the Service’s responsibility to assess threats to Canada and Canadians rigorously, and in a professional manner, and provide objective advice to Government based on those assessments. The Committee is fully in accord with initiatives to bring the respective skills of CSIS and the RCMP together on appropriate projects. At the same time, the Service also has responsibility to ensure that this advice is of the highest possible quality. The Sidewinder first draft report did not meet that standard, and renewed efforts succeeded in producing a much-improved final product.

Lost Documents—A Serious Breach of Security

Report #126

BACKGROUND TO THE INCIDENT

On October 10, 1999, the vehicle of a CSIS Headquarters employee was vandalized in the Greater Toronto area. Inside the vehicle were a number of CSIS documents, several of which were classified. These were among the items stolen. The police were notified when the break-in was discovered, and the employee later reported the theft to a supervisor at the Service.

The police investigation revealed that the theft had been committed by petty thieves intent on supporting a drug habit, and that in all likelihood they had discarded the classified documents unread in a garbage dumpster, which was subsequently emptied at a landfill site. The documents were not recovered.

Following an investigation by the Service's Internal Security Branch—standard procedure in such cases—the employee was dismissed from the Service and more minor administrative actions were taken against other Service officers tangentially involved in the incident. In addition, the Service altered some of its procedures for document control and strengthened its internal “security awareness” program.

The Committee's review encompassed all elements of the incident: the circumstances that led to the Internal Security investigation, the manner in which the investigation was carried out, the results it yielded and all factors that would aid in assessing whether the incident pointed to systemic security problems within the Service.

FINDINGS OF THE COMMITTEE

Was There Warning of the Employee's Inappropriate Behaviour?

Our review of the Service's security records showed no previous security violations by the employee beyond those of a minor nature. Nothing in CSIS files presaged the employee's behaviour and the serious security breach that ensued.

Potential Damage to the Service and to the Security of Canada

With a view to assessing the potential damage to national security should the classified documents be found and released, the Committee examined copies of the lost material. The Service's own damage assessment concluded that although some of the information in the reports was dated, or had already become public knowledge, the potential for damage was high. The information contained would have revealed the existence of certain CSIS investigations and, more critically in the Service's view, the nature of CSIS operational limitations. The Service's assessment noted two important factors serving to moderate the potential damage: no sources were identified nor were any operations compromised.

Based on our review of the documents, we concurred with the Service's view: the documents held the potential to expose the country unnecessarily to security threats.

Problematic document management

In the course of its investigation, Internal Security had considerable difficulty determining the precise content of one item, and thus had to make an educated guess at what the employee held at the time of the burglary. This apparent lapse helped nudge the Committee toward the conclusion that there may have been a problem in CSIS internal document control procedures generally. The Service's explanation for the gap in information was that at the time the document was removed from CSIS premises by the employee, it had not been entered into the corporate file system.

Although not directly related to this security breach, a second document control issue emerged subsequent to the incident. The Committee learned about a case of unauthorized possession of documents. After seeking explanations from two operational branches about their respective control procedures, the Service investigation concluded that the case was an isolated one and that no changes in procedure were required.

To prevent either problem from recurring, the Service has reiterated to its personnel the importance of following proper document control and authorization procedures.

Other Issues Raised by the “Lost Documents” Affair

As noted earlier, several other employees were involved—albeit peripherally—in the incident. Although the Service's internal investigation showed that most media allegations of procedural non-compliance were unfounded, in the Committee's opinion the incident highlighted a lack of rigour in the Service's control over the removal from its premises of documents by officers. The Service has since taken steps to address these gaps.

Policies and the Human Factor

It is evident to the Committee that institutional scrutiny of the incident by us and the Office of the Inspector General, intense media interest, and the Service's own inquiries drew unprecedented attention to the Service's internal security mechanisms. As a result, changes have been made. Nevertheless, it is CSIS' view—and we agree—that no amount of regulation or policy can rule out the possibility of such incidents occurring. Intelligent intelligence work ultimately depends on conscientious people, as well as on strict rules.

“LOST DOCUMENTS” MATTER IN PERSPECTIVE

Previous Internal Security Cases

As part of the Committee's review, we asked CSIS for information about previous internal security investigations and outcomes. Our analysis took into consideration the sea change in national and international security environments in the last fifteen years, and concomitant adjustments in CSIS policies and practices particularly in reporting security breaches.

Although we were unable to identify any single case identical to this most recent one, we did note that a wide range of penalties had been imposed on offending employees—including termination of employment—in cases that shared some of the same elements.

The Committee's review of security breach historical records gave rise to two observations. First, that changes to CSIS internal security policy and practices were often driven by security breach incidents, not considered analysis and review of procedures. The Service's approach to internal security was essentially reactive, notwithstanding internal and central Government agency policies that mandate periodic reviews.

Second, several of the cases in the Service's records have caused the Committee to consider new audit

and review procedures so as to ensure that Members have as complete an understanding as possible of such events, as and when they occur.

The Service's handling of the investigation

The Service's own “lost documents” investigation was conducted in a competent and professional manner, ultimately revealing how its classified materials went astray. Internal Security Branch staff maintained a focused and coordinated approach to handling the many issues and questions raised by the incident. CSIS Headquarters gave clear direction to Toronto Region which, in turn, successfully enlisted the very important co-operation of local law enforcement

No amount of regulation or policy can rule out the possibility of such incidents . . . intelligence work depends on conscientious people, as well as on strict rules

agencies—co-operation crucial to learning the probable fate of the documents. Finally, the policies and guidelines in place for performing and consolidating damage assessments by various operational branches proved effective.

CONCLUSION

As already noted, the Service's internal security policy framework has been in place for a number of years, with change usually stimulated by a security intelligence breach at home (“lost documents”) or abroad—the Aldrich Ames CIA case being one of the more notorious examples.

Although this most recent incident cannot be traced to faulty internal security policies, it has served to highlight a lack of rigour in certain of the Service's

procedures for implementing those policies. We are aware that the Service periodically conducts its own internal review of security procedures. Nevertheless, security breaches in recent years involving CSIS materials (and commented upon in these pages) suggests that these internal reviews have not been as effective as the Service and the Committee would have wished. The Committee will continue to monitor this area of Service operations closely.

Threats from a Foreign Conflict

Report #124

BACKGROUND TO THE STUDY

The focus of this study is a CSIS investigation of possible threats emanating from a conflict abroad. Canada is susceptible to the spillover from foreign wars and civil strife for a number of reasons: its open society and relatively porous borders, its activist international policies and robust defence alliances, and the presence in Canada of various “homeland” communities. It is in the nature of homeland conflicts that attempts are sometimes made by one or other of the warring parties to enlist the support (moral, political and financial) of compatriots in Canada.

In this instance, the perceived threat arose chiefly from the activities of foreign intelligence services operating in Canada. These included suspected attempts to raise funds, collect information on homeland communities, foment civil unrest in Canada, and illegally procure weapons and technology.

As with every review of a homeland conflict investigation, the Committee directs special attention to gauging the impact of the Service’s investigation on the homeland communities themselves. Whenever the Service targets domestic groups or conducts interviews within homeland communities, we wish to ensure that it acted appropriately and entirely within the law.

The audit covers the two-year period from April 1997 through March 1999. The Committee examined all the information generated and retained by the investigation, the targeting authorities requested and warrant powers obtained, and the use made by the Service of information from human sources including its community interviews.

FINDINGS OF THE COMMITTEE

The Committee determined that the Service had sufficient grounds to conduct the investigation and to employ the investigative methods permitted in the targeting authorities and Court warrants. The level of investigation was proportionate to the seriousness of the threat and, with one exception, only information strictly necessary to the investigation was collected.

Three issues drew the Committee’s attention:

- an overly general targeting authority;
- community interviews;
- retention of unnecessary information.

An Overly General Targeting Authority

The Service obtained two authorizations, and it was the second and most intrusive that raised some concerns. It set out to investigate the activities of foreign intelligence services, which could lead to the targeting of foreign diplomats and an individual resident in Canada thought to be associated with those agents. The intent was to learn the extent to which the intelligence officers or their associates were engaged in clandestine or illegal activities that constituted a threat to Canada.

Although the targeting authority in question stated that the investigation was required in order to assess three categories of threat—espionage, foreign influenced activities and politically motivated violence (subsections 2(a), (b) and (c) of the *Act*, respectively)—with one of the targets named in the Request for Targeting Authority (RTA), only one of the threat categories cited could reasonably be said to apply.

Current Ministerial Direction is careful to set various thresholds and standards that must be met for each type of threat. In the view of the Committee, all RTAs should specify how the threats any particular target is alleged to represent conform to these criteria.

The Committee recommends that RTAs be structured and written to identify clearly the reasons for targeting each target named, under each threat definition cited.

Community Interviews

In general, the Service's contacts with individuals of homeland communities were conducted appropriately. The Committee did identify one instance where a CSIS investigator appeared to counsel an individual about whether to organize or participate in public demonstrations. Nothing we learned about the matter led us to doubt the officer's good intentions, however, we urged CSIS to remind officers that their task is to gather information, not to offer political direction.

Retention of Unnecessary Information

The Committee's review of CSIS databases identified only one instance where the "strictly necessary" test for collecting information was not met. The information was clearly of a personal nature and had no investigative value. We strongly advised the Service of our concerns. The Service has agreed with this finding and ordered the information deleted from its database.

Terrorist Fundraising

Report #122

BACKGROUND

Beginning with the Halifax G8 Summit in 1995, the international community has paid increasing attention to the issues of illicit transborder fundraising in support of terrorism. In 1996, the G8 nations adopted a series of measures designed to curb the improper use of "organizations, groups or associations,

including those with charitable, social, or cultural goals, by terrorists using them as a cover for their own activities."⁶ With the same goal in mind, the United Nations is expected in 2000 to adopt the International Convention on the Suppression of the Financing of Terrorism.

Relative prosperity, openness and diversity make Canada an ideal place for organizations devoted to using terrorism to achieve political ends to obtain needed funds through illicit means. Although a number

Management of Targeting

Target Approval and Review Committee

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 that are related to, or emanate from, that specific issue.

of countries, including the United States and United Kingdom, have implemented legislation proscribing known terrorist organizations and criminalizing all of their fundraising activities, Canada, for various reasons, has refrained from taking a similar step.⁷

The Government's efforts to deal with this growing international problem have focused on more effective exchanges of information among Canadian agencies, and more stringent enforcement of existing laws and regulations. At the centre of the Government's new initiative was the creation in 1996 of the *Interdepartmental Working Group on Countering Terrorist-Support Activities* (IWG). This body brings the regulatory, investigative and information collection skills of the RCMP, Citizenship and Immigration Canada, the departments of Foreign Affairs, Transport, Justice, Finance, and National Defence—as well as CSIS—to bear on the problem of terrorist fundraising.

The Service plays an advisory role to the Government through the mechanism of the IWG, and provides information about alleged terrorist fundraising in Canada directly to the relevant federal departments. The purpose of the Committee's study was to examine several facets of the Service's work in addressing the problems of terrorist fundraising in Canada.

METHODOLOGY OF THE AUDIT

The Committee's audit encompassed three types of source data:

- all relevant files documenting communications and exchanges of information between CSIS and the Government of Canada for the period from March 1, 1995 through March 31, 1999;
- interviews with relevant CSIS officers and their interlocutors in various departments of government;
- a selected sample of relevant Service investigations were subject to a thorough review, including all

relevant targeting documents, operational files, warrant files and information received from foreign agencies.

Our goals were twofold: to determine the effectiveness of Service advice and co-operation in assisting the Government's efforts to curb terrorist fundraising, and to ensure that all CSIS actions were appropriate and in conformity with the law.

FINDINGS OF THE COMMITTEE

Service Investigations of Terrorist Fundraising

The Service stated that, as a result of its investigations linked to international terrorism, it had uncovered several Canadian organizations suspected of facilitating terrorist fundraising objectives. Our own review of these investigations showed that CSIS did have sufficient information to believe that the links to international terrorist groups and to their fundraising efforts constituted a threat to the security of Canada.

Information-sharing

Information-sharing between CSIS and client departments has been ongoing for some time, although the Committee noted that a hiatus in relations with one department lasted several months. The lines of communication with that department have remained open ever since. CSIS and its departmental clients both expressed satisfaction with the liaison relationship. Recipients of Service reports said that the information had been most useful as “investigative leads” assisting in determining how and where to follow up.

The Committee's review of the information-sharing process identified a number of difficulties and potential obstacles:

- the use of CSIS information in court proceedings;
- the nature of the advice to government.

The Use of CSIS Information in Court Proceedings

In providing information to client departments, the Service has experienced problems handling information of potential evidentiary value similar to those the Committee has encountered in other CSIS liaison relationships.⁸ Current Canadian law makes it difficult to protect classified intelligence from disclosure in legal proceedings where the information is used to support prosecution. CSIS is concerned to protect domestic and international sources and, in the absence of modifications to current law, client departments' ability to use the Service's information in court will continue to be constrained.

The Nature of the Advice to Government

After examining CSIS files, the Committee noted that the Service was selective in the information it gave to the client departments. In response to a query from the Committee, the Service stated that it refrained from distributing information that could adversely impact the security of human sources, Service operations or relations with third parties, for example allied intelligence agencies.

RECOMMENDATIONS

Two recommendations emerged from this study. First, in respect of the nature of the Service's advice,

The Committee recommends that in future, CSIS advise its client departments of substantive changes to the assessments it has previously given them, which arise as a consequence of new information.

Second, although the Committee supports legislative changes that would allow more effective use to be made of the information shared between CSIS and its client departments, such enhanced procedures could well generate an increase in the number of complaints brought to the Committee. To address such an eventuality,

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 social 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.

The Committee recommends that the Ministry of the Solicitor General and Privy Council Office initiate special measures to keep SIRC apprised, on a timely basis and as appropriate, of the IWG's proposals as they impact on CSIS activities.

The Committee will continue to monitor the Service's role in providing advice to the Government of Canada about this growing threat to Canada's security and Canadian interests.

Investigation of a Domestic Threat

Report #121

METHODOLOGY OF THE AUDIT

During a previous review, the Committee learned of several CSIS source operations that sometimes involved the legitimate dissent milieu—specifically,

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 denying 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.

certain protests and demonstrations. We subsequently conducted a review of the investigations.

Under the terms of the authorizations for the investigations, several individuals were targeted under sections 2(c) and 12 of the *CSIS Act* wherein the Service has the responsibility to investigate threat activities "directed to or in support of the threat or use of acts of serious violence against persons or property for the objective of achieving a political objective within Canada or a foreign state . . ."

During its investigation, CSIS collected information about the targets, as well as some information about protests and demonstrations in which the targets were

involved. Information the Service obtained was used in threat assessments given to federal government clients and relevant law enforcement agencies.

During the Committee's review of the investigation—and with particular reference to CSIS policy and Ministerial Direction concerning legitimate advocacy, protest and dissent—the Committee examined all reporting by CSIS sources, all information retained on targets and protests and other incidental intelligence collected. We reviewed all relevant targeting authorities, source handling files and Service internal memoranda. In addition, the Committee interviewed CSIS personnel responsible for the investigations.

FINDINGS OF THE COMMITTEE

The Committee's review identified no violations of Service policy or Ministerial Direction. CSIS had reasonable grounds to suspect that the targets were threats to the security of Canada. None of the human sources engaged in illegal or *agent provocateur* activities, and the sources gathered information on appropriately approved targets. We saw no instances of influence by CSIS sources on the activities of legitimate groups or organizations.

Notwithstanding our general conclusions, this set of investigations was the source of some residual concerns for the Committee. During the course of investigations, which lasted several years, the Service made targeting decisions, chose investigative methods, collected information and advised government clients—all actions carried out in accordance with policy as written—which when reviewed as a whole left the Committee uneasy. Among these were:

- existing policies for managing human source investigative techniques did not ensure that executive management was fully seized with the fact that, because of unforeseen activities of the authorized targets after the original TARC approval, an organization not itself an authorized

target had become implicated in the Service's investigative activities;

- CSIS instructions that sources were only to report on “authorized subjects of investigation” was not fully implemented in practice in some instances;
- in two instances while conducting surveillance of authorized targets, the Service inadvertently collected some information on the activities of an organization. The Service did not retain the information in its active database;
- one threat assessment issued by the Service based on information gathered during these investigations did not, in the Committee's view, accord with the intent of the *Act*.

The Committee believes that these instances—admittedly few in number—point to an occasional lack of rigour in the Service's application of existing policies, which oblige it to weigh the requirement to protect civil liberties against the need to investigate potential threats. We brought these particular instances, and the Committee's overall concern about the need for rigorous weighing, to the attention of the Service.

In the Service's view, its existing policies, including the need for multiple levels of approval, adequately address the Committee's concerns. It believes it is in full compliance with Ministerial Direction which requires it to choose investigative methods and techniques proportionate to the threat, and to ensure that these are weighed against possible damage to civil liberties. The Service stated that “. . . the position that the [CSIS] *Act*, in combination with Ministerial Direction, requires evidence of ‘weighing’ in every single case before a targeting approval is given, is a distortion of both the *Act*, and of Ministerial Direction.”

The Committee is in no doubt that, in all of its investigative activities, the Service takes the matter of civil

liberties extremely seriously. However, with respect to its position on the need for evidence of weighing in “every single case,” we disagree.

It is an essential principle of administrative accountability that the processes by which judgements and decisions are made can be as important as the decisions and outcomes themselves. The Committee would like to see tangible evidence that significant investigatory decisions involving the legitimate dissent milieu are adequately weighed.

The Committee recommends that the Service make the changes to its administrative procedures necessary to ensure that all significant investigatory decisions in the area of lawful advocacy, protest and dissent are weighed and so documented.

The Committee believes that as well as providing an additional measure of comfort to the Review Committee, such changes would help maintain the day-to-day sensitivity of all CSIS staff to the need to protect civil liberties.

The Committee had an additional recommendation concerning the need to clarify a section of the CSIS *Operational Policy Manual* (a classified document).

A Long-Running Counter Intelligence Investigation

Report #118

BACKGROUND TO THE REVIEW

The Review Committee believes that an essential aid to ensuring the continued quality and appropriateness of CSIS activities is the periodic review of major investigations that span a number of years. We last reported on this counter intelligence operation some time ago.

AUDIT METHODOLOGY

The Committee's inquiries and research were designed to answer certain key questions about the investigation:

- Did a threat (as defined in the *CSIS Act*) in fact exist?
- Was the nature of the Service's investigation (the level of intrusiveness, the quantity of resources deployed) proportionate to the threat?
- Were CSIS actions appropriate, in compliance with Ministerial Direction and internal policy and within the law?
- Was the advice given to the Government based on the investigation timely, balanced and accurate?

Our audit encompassed CSIS operational files for a selected set of investigations, documents supporting targeting requests and warrant applications, Service reports generated for clients throughout the Government and interviews with CSIS officers and with consumers of Service intelligence products in other departments of Government.

In addition to reviewing specific Service activities, the Committee took into account such factors as the

number of known and suspected intelligence officers in Canada, and less tangible factors such as the potential damage to Canadian interests should allied governments come to believe that Canada's counter intelligence efforts were inadequate or ineffective.

FINDINGS OF THE COMMITTEE**The Nature of the Threat**

It is the Service's view that the target of this investigation is engaged in intelligence-related activities that manifest themselves in classical espionage, foreign influence in various aspects of Canadian society and the theft of economic and scientific information through clandestine means.

In an earlier report the Committee stated that "the threats posed by the intelligence gathering activities of this [target] [were] at th[e] time, nebulous, and sometimes hard to define." Although events since then have served to confirm that the potential for serious threat to Canadian interests is serious and genuine, the current threat as measured in concrete and confirmed activity appears to us to be limited and infrequent.

This difference of opinion between CSIS and the Committee about the nature of the threat led us to conclusions about some of the target's activities that were at odds with those of the Service. Some of the activities investigated by the Service showed the target engaged in intelligence gathering in Canada, but others did not.

In one case the Service treated as a threat activity—an attempt to influence a Canadian official—what seemed to be routine diplomatic behaviour. In another, with little corroborating information, CSIS ascribed intelligence gathering motives to apparently normal consular contacts.

The Committee's review also raised questions about some beliefs the Service has about the nature of the

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.

threat. We are of the opinion that these beliefs are sometimes overdrawn.

Targeting Decisions

The Review Committee thoroughly examined a representative selection of Service targets approved for investigation by the CSIS Targeting and Review Committee. We reviewed the case the Service set out for each and studied warrant affidavits, supporting documentation and reports generated by the investigations.

The Committee believes each of the targeting decisions examined was justified by the evidence. However, in the Service's application to secure warrant powers against one target were a number of overstatements. In one instance, information put forward was more than a decade old and the information adduced was derived from one source's "feelings." In another, a source's speculation was quoted. Some assertions that the target engaged in "suspicious activities" appeared to us to be misleading or exaggerated. Despite these imprecisions, however, the Committee believes the evidence to proceed with targeting the individual was convincing overall.

Investigative Activities and Retention of Information

The Committee identified several instances in which the Service acted in contravention of policy or without due caution:

- some information collected by the Service did not meet the "strictly necessary" test: a membership list, reports about a public meeting and particulars about individuals who were neither targets themselves nor known to have contacts with targets;
- Service actions in regard to one target appeared to carry significant risk;
- CSIS files about one aspect of an investigation appeared to show that a source rendered assistance

to a target in a manner that gave rise to the Committee's concern.

Employment of Resources

The Committee was at pains to assure itself that the resources devoted by the Service to this investigation were appropriate to the threat. While our review turned up no acute difficulties, we will continue to monitor the Service's deployment of resources in this area.

Advice to Government

The Service produces several classified publications to transmit its findings to various readerships in the Government of Canada. The Committee examined a selection of CSIS publications relating to this particular investigation, compared the statements in them to supporting information in Service files, and asked clients their views of the utility and accuracy of Service reports.

None of the clients we interviewed took issue with the accuracy, timeliness or analytical quality of the reports they received. Most considered the Service's reports to be useful background information. The Committee's review of the information in support of Service conclusions in selected CSIS reports did, however, reveal some anomalies:

- the Service stated that an action by a target was possibly for the purpose of "developing a network of agents." Our review showed that there was no documentation on file to support this premise;
- a report stating that a target had used a certain business practice to obtain proprietary advanced technology was not technically correct. In our view, the Service's information differed from the report's description;
- CSIS informed its readers that a target had engaged in a number of instances of "espionage" over a long period. In examining these instances, the Committee formed the opinion that the

evidence for some was weak, speculative or ignored reasonable, benign alternative explanations for the actions in question.

CONCLUSION

The Committee believes that the potential threat to Canadians and Canadian interests arising from the activities of this target is significant. It is vital, therefore, that the Service take special care to ensure that the analysis and reporting generated by its investigations remain precise and unbiased. The Government of Canada faces a myriad of difficult international security, economic and diplomatic issues. It deserves the best possible national security advice—clear in analysis, as transparently obtained as law and prudence permit

The Government deserves the best possible national security advice . . . as transparently obtained as law and prudence permit and unencumbered by unfounded speculation

and unencumbered by preconceptions or unfounded speculation. Our review evidenced a few instances that pointed to the Service occasionally drawing conclusions not based on the facts at hand.

Domestic Exchanges of Information (4)

Report #119

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. The Service's mandate to enter into such arrangements is set out in section 17 of the *CSIS Act*.

The Service discloses information to various domestic departments and agencies “for the purposes of the performance of its duties and functions” under section 19(2) of the *Act*.

Under section 38(a)(iii) of the *Act*, the Committee is charged with the task of examining the co-operation arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

METHODOLOGY OF THE EVALUATION

This review focused on CSIS' domestic exchanges of information for calendar year 1998. In addition to reviewing the Service's information exchanges in all regions, the Committee also conducted an on-site review of one regional office.

The purpose of the review was to assess whether CSIS had adhered to its arrangements with the other agencies, and whether it had collected and disclosed information in compliance with the *CSIS Act*, Ministerial Direction and CSIS operational policies. In particular, the Committee's enquiries were meant to determine if:

- the threat was balanced with the infringement on personal privacy resulting from the passage of the information;
- the exchange of information was strictly necessary to meet the Service's operational requirements as per section 12 of the *CSIS Act*;
- the exchange of information involved the unnecessary use of personal and sensitive information;
- the information exchanged was reasonable and factually accurate;
- all CSIS disclosures of information were in accordance with the preamble to subsection 19(2) of the *CSIS Act*.

COMMITTEE FINDINGS

Overall Co-operation

The Committee found that CSIS co-operation with federal departments and agencies and its relations with provincial authorities and police forces was productive. Our review also showed a general willingness between CSIS and the RCMP to share information with each other.

In one region, however, the Committee found a list of outstanding requests for information from the RCMP. We questioned the delay and learned that the region had since implemented a tracking mechanism in an effort to deal with the problem.

Exchanges and Disclosures of Information

Although the Committee found that the majority of CSIS exchanges of information in 1998 complied with policy, agreements and statutory requirements, we found some instances where, in the Committee's opinion, CSIS had retained unnecessary information.

Unnecessary Retention of Information

The Committee found that one region had collected a report that did not meet the "strictly necessary" criterion under section 12 of the *CSIS Act*. CSIS has since removed the report from its database.

In another instance, our on-site audit of one CSIS region revealed that it had retained several reports in its operational database that it had received from two agencies about planned protests and demonstrations.⁹ In our view, some of the information contained in the reports did not demonstrate reasonable grounds to suspect serious violence or a possible threat to public safety. The Committee recommended that CSIS report and retain only the information required to meet its obligations with regard to threat assessments.

The Tracking System

The Committee found that, in general, CSIS' tracking of information exchanges with domestic agencies was

consistent. However, we did note variations in how the regions applied the tracking procedure, and a few cases in which the tracking information was not accurately recorded. We also expressed our concern about the fact that the policy on operational reporting was still under development for an inordinate length of time.

Proliferation of Weapons of Mass Destruction

Report #120

BACKGROUND TO THE STUDY

Canada's efforts to prevent or at least slow the proliferation of weapons of mass destruction (WMD)—chemical, biological and nuclear—to states that do not possess them are longstanding. Since the end of the Second World War, Canada has been at the forefront of every important diplomatic and political initiative aimed at creating an international regime to monitor and control the spread of such weapons, the means for delivering them and the technologies needed to build them.

Since the demise of the Soviet Union, the threat to Canadians' security from such weapons has become more diffuse and also more difficult to counter. Growing numbers of states, and even terrorist organizations, are gaining the wherewithal to purchase (or in some cases steal) the technologies and expertise needed to manufacture extremely lethal weapons that could be used against Canada or its allies.

Although Canada does not possess such weapons itself, a national infrastructure of advanced nuclear, chemical, biotechnological and electronic industries and research facilities makes the country vulnerable to illicit procurement. Many technologies used domestically for peaceful endeavours can also be used in weapons manufacture—so called "dual-use" technologies.

Stemming the improper flow of WMD and their supporting technologies has been a pillar of Canada's

foreign policy for many years. An important domestic element of this policy is the need to understand the nature of illicit and clandestine activities that may pose a threat to the security of Canada, Canadians and others. The Service has an important role in collecting and analyzing such information, stating in 1999 that “counter proliferation is one of its security intelligence priorities.”¹⁰ The goal of the Committee’s review was to assess the Service’s performance of its function to advise the Government in a clearly vital area.

The Service correctly viewed the target’s efforts to circumvent Canada’s laws as a threat to national security

METHODOLOGY OF THE AUDIT

The Committee reviewed all files for fiscal years 1997–98 and 1998–99 held by the Service in relation to its issue-based investigation of WMD proliferation. We interviewed Service personnel, attended briefings and examined CSIS Target and Review Committee (TARC) documents in cases representative of the Service’s entire counter-proliferation effort. In addition, the Committee examined a number of cases that gave insight into the Service’s Counter Proliferation Unit, its methods of operation and its relationship with domestic and foreign agencies.

FINDINGS OF THE COMMITTEE

Threat from a Foreign Country

From CSIS files it was evident that, because of consistent attempts to procure WMD, a certain foreign country was a particular focus for the Service’s investigative efforts. Based on an extensive review of the documentation, we concluded that CSIS had reasonable grounds to suspect a threat to the security of Canada

under sections 2(a) and (b) of the *CSIS Act* and that the targeting level for the investigation was proportionate to the threat. The Committee determined that with one exception (which we brought to the Service’s attention), the information collected met the “strictly necessary” test.

Threat from a Particular Target

The Committee examined the case of a particular counter-proliferation target that had recently come to our attention. We believe the Service correctly viewed the target’s efforts to circumvent Canada’s laws as a threat to national security.

Certain Illegal Activities

The Service received information that led it to believe some activities had taken place that constituted a threat to the security of Canada as defined in sections 2(a) and (b) of the *Act*. Subsequent CSIS investigation revealed that a violation of Canadian law had occurred and the appropriate department of the Federal Government was so advised. The Committee found that the level of investigation employed by the Service was proportionate to the threat and that CSIS had retained only strictly necessary information in its database.

The Service’s Counter-proliferation Effort in General

It is evident to the Committee that the Service plays an important role in Canada’s management of proliferation issues at the domestic level (co-operating with police and other enforcement agencies), and globally (acting in support of DFAIT counter-proliferation initiatives, and exchanging information with allied governments and other parts of the international antiproliferation regime). We noted that, overall, the Service’s approach to proliferation matters was both strategically sound and flexibly managed. The Service was particularly concerned to give the counter-proliferation unit considerable leeway in its staffing decisions, reflecting the specialist and technical nature of the tasks being pursued.

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

Report #123

Every year the Committee audits the entire range of the CSIS investigative activities—targeting, special operations, 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 main questions:

- 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 information that was strictly necessary to report or to advise the government on a threat?

METHODOLOGY OF THE AUDIT

In the region at issue, the Committee selected nine investigations at random—five counter terrorism cases and four counter intelligence cases. We reviewed all files and operational messages in the

Service's electronic database and interviewed the regional managers who oversaw the investigations.

FINDINGS OF THE COMMITTEE

In all nine cases, the Committee found that CSIS had reasonable grounds to suspect a threat to the security of Canada. The levels of investigations were proportionate to the threat-related activities of the targets and the Service collected only the information that was strictly necessary to advise the government. During the course of the audit, two counter intelligence investigations, one of quite long-standing, were terminated. Based on our review of the intelligence collected during the period under review, the Committee concurred with the Service's decisions in both cases.

Two of nine investigations we examined did raise matters of concern:

- An instance where the request for targeting approval presented a fact inconsistent with the

The Warrant Process

To obtain warrant powers under section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court with a sworn affidavit justifying the reasons why such powers are required to investigate a particular threat to the security of Canada. The preparation of the affidavit is a rigorous process involving extensive consultations with the Department of Justice, and the Solicitor General, with the latter's approval being required before a warrant affidavit is submitted to the Court. The facts used to support the affidavit are verified during the preparation stage and reviewed again by an "independent counsel" from the Department of Justice to ensure that the affidavits are legally and factually correct prior to their submission to the Federal Court. This process has evolved over the past several years with a view to ensuring that the facts, and statements of belief based on those facts, are accurate.

information the Service had collected. Although the Committee determined that the discrepancy did not undermine the legitimacy of the targeting authorization, we again emphasized to the Service its ongoing responsibility to ensure that facts presented in requests for targeting accurately reflect the information it holds.

- Contrary to the Service's operational policy, the regional office failed to submit an assessment report following the termination of a counter terrorism investigation. The Service attributed the lapse to an administrative oversight and has taken measures to prevent a reoccurrence.

Obtaining and Implementing Federal Court Warrants

Under section 21 of the *CSIS Act*, only the Federal Court of Canada can grant CSIS the right to use warrant powers, such as telephone or mail intercepts. In requesting such powers, the Service must present an affidavit to the Court attesting to the facts that require their use. As part of its regional audit, the Committee reviewed how the Service implemented the warrants obtained in that region. Our goal was to ensure the Service's compliance with all warrant clauses and conditions.

FINDINGS OF THE COMMITTEE

Warrant Implementation

The Committee reviewed all active warrants in the Region during the period under review. In one of the warrants reviewed, the Service's implementation of warrant powers was limited to intercepting a target's telecommunications. In another, CSIS elected not to make use of any of the powers granted to it. The Service decided not to seek a renewal of either warrant and ultimately terminated the investigations.

The files we examined disclosed a number of minor procedural discrepancies: an unusual delay in submitting certain reports required upon termination of an investigation, the inappropriate use of tracking and date codes on intercept reports and the failure to convene a formal "tasking meeting" as required by Service policy.

Although these issues may appear to be of little consequence, the Committee believes that disciplined logging, reporting and tracking procedures are essential if intelligence gathering is to be effective and at the same time accountable.

Quality Control in Reporting

Because intercept reports can provide the basis for requests to continue warrant operations and for the granting of new targeting authorities, accuracy in transcribing such material is vital. This year's regional audit showed that in accordance with 1997 draft policy, the region in question was conducting the appropriate quality control checks.

Audit of Sensitive Operations

The very nature of sensitive operations dictates that they are subject to 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 require the approval of Service senior management.

METHODOLOGY

For the purpose of this regional audit, the Committee examined a set of randomly selected human source operations. In addition, we reviewed all requests to senior managers involving "sensitive institutions."¹¹

FINDINGS OF THE COMMITTEE

In general, the Committee concluded that the region's development and direction of sources were appropriate. However, we identified a number of shortcomings in

the Region's compliance with policy and established administrative procedures.

- A situation with the potential to bring discredit to the Government of Canada was not reported to the Deputy Director of Operations in accordance with operational policy.
- The regional office under review failed to obtain formal prior approval from Human Sources Branch before directing a source to travel to another region for the purpose of providing operational assistance to that regional office.
- For what the Committee regards as an unnecessarily extended period, a Regional Office failed to complete an important form required by policy. While satisfied with the measures taken by the Region to rectify the problem, we believe that the Service should have taken measures earlier to ensure compliance.
- The Region was consistently late in providing certain reports, reviews and forms to CSIS Headquarters. The Service stated that its recent implementation of a new tracking system had eliminated the gaps in filing.

Internal Security

The Committee's audit of security procedures in the office under review identified two potentially serious matters. Timely intervention by management in the Region ensured that the incidents did not escalate and that more serious violations were averted. We determined that the office's internal security practices and procedures were generally sound and noted that in response to incidents elsewhere in recent years, the Region had implemented CSIS Headquarter's new procedures in relation to managing classified documents and electronic storage media.

The Committee did note, however, that the Region had conducted significantly fewer (in proportion to the staff complement) random searches of employees entering or leaving Service premises than CSIS offices in other regions. Given the security breaches of recent years, and the Service's acknowledgment of the role of random searches in increasing "security awareness" among its employees, the Committee believes the Region should bring its security practices into line with other of the Service's regional operations.

The Committee recommends that the Region increase the number of random searches to reflect the current practices in other CSIS regional offices.

C. Inside CSIS

Warrants and Warrant Statistics

Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone their use bears continued scrutiny, a task the Committee takes very seriously. In addition, the review process provides insight into the entire breadth of CSIS investigative activities and is an important indicator of the Service's view of its priorities.

The Committee compiles statistics based on a quarterly review of all warrant affidavits and warrants granted by the Federal Court. Several kinds of information are tracked annually, such as the number of persons and number of locations subject to warrant powers. Table 1 compares the number of warrants over three fiscal years.

The Service did not seek renewal of any of its warrants during 1999–2000. The Federal Court issued 29 urgent warrants; however, none were renewed or replaced

during this same fiscal year. As of March 31, 2000, CSIS had in place a total of 238 warrants.

FINDINGS OF THE COMMITTEE

Although the data provides the Committee with an excellent profile of the Service's requests for warrant powers in a given year, comparisons year-to-year are less enlightening because the applications vary as a result of decisions by the Court and new kinds of powers sought. In addition, raw warrant numbers can be misleading because a single warrant can authorize the use of warrant powers against more than one person.

Allowing for these factors, the Committee concluded that the total number of persons affected by CSIS warrant powers remained relatively stable for the last two years and that foreign nationals continue to represent the overwhelming majority of persons subject to warrant powers.

REGULATIONS

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies for warrants. In 1999–2000, no such regulations were issued.

FEDERAL COURT DECISIONS

None of the applications for, or execution of, certain powers contained in warrants were affected by Federal Court decisions in fiscal year 1999–2000.

Although no applications for new warrants were denied, the Federal Court of Canada in June 1999 declined to issue two replacement warrants based on an interpretation of paragraph 21(2)(a) of the *CSIS Act*. The Service reapplied to the Federal Court and the warrants were approved one month later. The first interpretation has not been adopted by the other designated judges.

WARRANT REVISION PROCESS

In last year's annual report, the Committee reported that, in 1998–1999, CSIS had begun a complete review of clauses and conditions in all existing warrants, with proposed changes to be approved by the Federal Court. During the period 1999–2000, CSIS completed the warrant revision process, and all changes reflected in subsequent warrant applications have been approved by the Federal Court.

CSIS Operational Branches

COUNTER TERRORISM BRANCH

The Counter Terrorism (CT) Branch is one of the two main operational branches at CSIS (the other being Counter Intelligence). Its role is to provide the Government of Canada with advice about emerging threats of serious violence, and about activities by foreign states or their agents in support of serious violence, that could affect the safety and security of Canadians and of Canada and its allies.

Table 1
New and Renewed Warrants

	1997–98	1998–99	1999–2000
New Warrants	72	84	76
Warrants Replaced/Renewed ¹²	153	163	181
Total	225	247	257

The threat from international terrorism continues to be associated with what are termed “homeland” conflicts. Various domestic extremist groups are also regarded as potential threats to the security of Canada because of their capacity to foment violence.

Although the Branch reported that its focus and priorities remained relatively unchanged for much of the 1999–2000 fiscal year, the arrest of Ahmed Ressay in the United States for transporting bomb-making materials from Canada prompted the Service to refocus its efforts on the emerging threats of serious violence.

Threat Assessments

CSIS provides threat assessments to departments and agencies within the Federal Government based on relevant and timely intelligence. CSIS prepares these assessments upon request or on an unsolicited basis—dealing with special events, threats to diplomatic establishments in Canada, and other situations.

In 1999–2000, the Threat Assessment Unit produced a total of 524 assessments, down from 683 the year previous. The Committee recognizes that many factors influencing these numbers—the number of foreign visitors to Canada, requests received from other Government departments and agencies, special events and threats identified during the year—are beyond the control of the Service.

COUNTER INTELLIGENCE BRANCH

The Counter Intelligence (CI) Branch monitors threats to national security stemming from the espionage activities of other national governments’ offensive intelligence agencies in Canada.

In last year’s annual report, the Committee commented on the lack of training for CSIS intelligence officers in the area of transnational criminal activity. CI Branch has since sought enhanced training of its investigators in three specialized fields: counter proliferation, information operations and transnational criminal activity.

The Service reported mixed success in its efforts to explore common ground for co-operation and information-sharing with certain foreign intelligence agencies. On the domestic side, the Service claimed several successes in forging co-operative relationships with other government departments.

In co-operation with a federal department, the activities of a foreign intelligence agency in Canada were curtailed, and a formal section 17 co-operation agreement with another intelligence agency was brought closer to conclusion.

REQUIREMENTS, ANALYSIS & PRODUCTION BRANCH

The Requirements, Analysis & Production (RAP) Branch provides advice to government on threats to the security of Canada through *CSIS Reports*, *CSIS Studies* and *CSIS Intelligence Briefs*. In addition, the Service published a number of unclassified reports in its *Perspectives* and *Commentary* series.

In 1999–2000, RAP produced a total of 48 reports, a decline from 68 issued the previous year. Recent years have seen a downward trend in the number of reports produced.

CSIS also contributes to the intelligence community through its participation in the Intelligence Assessment Committee (IAC)—a body made up of senior officials from those departments and agencies of the Government of Canada most concerned with intelligence matters. During the past year, the Service took the lead in seven IAC reports and contributed to another nineteen.

In last year’s annual report, the Committee presented the findings from an extensive review of the Branch. Among the Committee’s recommendations was that the defunct Executive Intelligence Production Committee (EXIPC)¹³ be reconstituted to help ensure that intelligence production was consistent with the requirements and priorities of the Government overall,

as well as with the needs of specific government clients. In 1999–2000, an EXIPC meeting was convened on one occasion and we hope this practice will continue.

Arrangements with Other Departments and Governments

CSIS RELATIONS WITH THE RCMP

The mechanisms to facilitate liaison and co-operation between CSIS and the RCMP are set out in the Memorandum of Understanding (MOU) between the two agencies. They include the assignments of liaison officers to both national headquarters and to each other's regional offices.

The Committee learned of several new initiatives to improve liaison and co-operation between the two agencies:

- the development of a staff exchange program;
- increased sharing of technical information and greater emphasis on the holding of joint training courses, presentations and conferences;
- the establishment in a region of a liaison committee tasked with addressing matters arising from the co-operation arrangement;
- implementation in a region of a tracking/diary date system to ensure that all RCMP requests for disclosure were followed up in a timely fashion.

The two organizations exchanged a total of 1518 documents in fiscal year 1999–2000. CSIS was responsible for providing more than half of the total (892). The Service also gave the RCMP 336 disclosure letters¹⁴ and 39 advisory letters.¹⁵

Implications of an RCMP Internal Audit

Last year, the Committee stated that it would examine the results of a then upcoming RCMP internal audit¹⁶

for their potential impact on Service activities. The RCMP's review included an examination of the CSIS–RCMP Memorandum of Understanding, and the functional working relationship between the two agencies.

The audit raised issues and problems similar to those examined in three of the Committee's own reviews:¹⁷ tension between the two agencies regarding disclosure, possible overlap in investigating transnational criminal activity and misunderstandings in each agency about the other's mandate.

Among its recommendations, the RCMP report proposed several mechanisms to help the RCMP and CSIS better understand each other's roles and limitations. The report also recommended changes to the MOU dealing with disclosure issues and the importance of employing the Liaison Program to resolve conflicts between the two agencies.

Coincident with the internal audit, the Service embarked on several initiatives aimed at improving its working relationship with the Force. These initiatives included:

- resuming the meetings of the Senior Liaison Committee. Originally established as a forum to resolve problems and disagreements between the two agencies, the liaison committee had been inactive since 1993;
- raising the level of the CSIS liaison officer position to that of the RCMP counterpart so as to promote the working relationship and signal the importance of the position within the Service.

Stinchcombe and the CSIS–RCMP Memorandum of Understanding

In the past, the Committee has commented on concerns expressed by both CSIS and the RCMP that the existing MOU did not adequately address issues of disclosure of CSIS information to the Courts arising from the

Stinchcombe decision. The Service informed the Committee that it is currently negotiating possible changes to the MOU with the RCMP in this regard.

DOMESTIC ARRANGEMENTS

In carrying out its mandate, CSIS co-operates with police forces, and federal and provincial departments and agencies across Canada. Pursuant to section 17(1)(a) of the *CSIS Act*, the Service may enter into co-operation arrangements with domestic agencies after having received the approval of the Minister.

CSIS currently has 19 formal MOUs with Federal Government departments and agencies and 8 with the provinces. CSIS also has a separate MOU with several police forces in one province. The Service signed no new MOUs with domestic agencies in fiscal year 1999–2000, nor were any existing arrangements with federal or provincial departments amended or terminated. The Service did receive Ministerial approval to negotiate an agreement with a provincial agency to conduct security assessments.

FOREIGN ARRANGEMENTS

Pursuant to subsection 17(1)(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General—after he has consulted with the Minister of Foreign Affairs—to enter into an arrangement with the government of a foreign state or an international organization. During the initial phases leading to the approval of an arrangement, CSIS is not permitted to pass classified information to the foreign agency. However, it may receive unsolicited information.

As of March 31, 2000, CSIS had 217 liaison arrangements with 130 countries. Of this total, the Service judged 45 to be “dormant.”¹⁸ During fiscal year 1999–2000, CSIS received the Minister’s approval for five new liaison arrangements, with the Minister turning down a Service request to expand the scope of an existing arrangement because of that country’s unstable political environment. Nine other arrangements were amended so as to broaden the

scope of information exchange, and the Service had 10 new arrangements under consideration.

An issue about which the Committee expressed concern in last year’s annual report was resolved. In a review of the agreement that set out the terms of a particular foreign liaison arrangement, we noted that a single generic name used in the text in fact represented several different intelligence organizations within the foreign state concerned—in the Committee’s view, a contravention of Ministerial Direction. The Service confirmed to the Committee that the Minister had been advised and the clarification noted. Only after these measures did active co-operation with the agencies begin.

MINISTERIAL DIRECTION

The Committee continues to regard the imminent release of a new Ministerial Direction on foreign arrangements as vital. Critical elements of the existing direction are outdated and the number of agreements between CSIS and foreign agencies during the past several years has increased dramatically. As of March 2000, no new Ministerial Direction had been forthcoming from the Solicitor General. However, we were again informed that the new Ministerial Direction is expected to be signed in the near future.

Collection of Foreign Intelligence

Report #117

Under section 16 of the *CSIS Act*, the Service—at the written request of the Minister of Foreign Affairs and International Trade (DFAIT) or the Minister of National Defence (DND), and with the written consent of the Solicitor General—may collect foreign intelligence. Under the *Act*, CSIS can make warrant applications for powers such as telephone intercepts and undertake other investigative activities at the request of these ministers.

Foreign intelligence refers to information or intelligence about the “capabilities, intentions or activities” of a foreign state. The *Act* stipulates that the Service’s collection of foreign intelligence must take place in Canada and cannot be directed at citizens of Canada, permanent residents or Canadian companies.

METHODOLOGY OF THE AUDIT

The Committee’s review encompasses all Ministerial “requests for assistance,” all information about Canadians retained by CSIS for national security purposes and all exchanges of information with the Communications Security Establishment (CSE) in the context of foreign intelligence.¹⁹

The goal of the audit is to:

- assess CSIS involvement in section 16 requests so as to ensure compliance with the *CSIS Act*, directions from the Federal Court and the governing Memorandum of Understanding (MOU);
- determine whether the Service has met the various legal conditions necessary to collect information under section 16 operations;
- assess whether the nature of the Service’s co-operation with the CSE is appropriate and in compliance with the law.

FINDINGS OF THE COMMITTEE

Ministerial Requests

A 1987 tri-ministerial MOU stipulates that any section 16 request likely to result in the inadvertent interception of communications to which a Canadian is party, should so state.²⁰ In last year’s report, the Committee noted that some requests for assistance had not contained the required cautions and caveats about the targeting of, or the inadvertent collection of

information about, Canadians. Although all Ministerial requests since August 1998 have contained such clauses, the Committee believes the declaration used currently concerning incidental interception requires additional clarification.

The Committee recommends that in requesting section 16 assistance, Ministers indicate explicitly those instances where there is a real likelihood that the communications of Canadians will be subject to incidental interception as part of the collection activity.

A related concern arises with respect to CSIS warrant applications resulting from section 16 requests. Two applications examined by the Committee did not include, as stipulated in the tri-ministerial MOU, the mandatory caution against directing the collection of information at citizens, companies and permanent residents.

The Committee strongly recommends that all future CSIS section 16 warrant applications contain the required prohibition against directing the collection of information at Canadian citizens, companies or permanent residents.

Retention and Reporting of Foreign Intelligence Information

The retention and reporting of information pertaining to Canadians, and collected by CSIS under section 16, continues to be of concern to the Committee. To ensure that no inappropriate data were retained in Service files or reported to other agencies, the Committee examined the special database holding foreign intelligence. In a few instances, in the Committee’s opinion, information went beyond the definition of foreign intelligence as set out in policy and law and included information that identified

Canadians or gave information about their activities that had very little intelligence value. In one instance, the Service agreed and the information was removed.

It is the clear intent of the *Act* and of existing policy that, in the process of gathering foreign intelligence, the Service take steps to ensure that the collection of information about Canadians be kept to an absolute minimum. In this regard, the Committee had some concerns about the length of time the Service retained certain information; about 10 percent of its foreign intelligence records contained references—some five years old or more—to Canadian citizens or landed immigrants.

The Committee raised the matter with the Service, which stated in response that schedules for retaining and disposing of information already collected are set out in the *National Archives Act* and that it was in compliance with those rules.

The Committee also reviewed CSIS reports to requesting Ministries based on section 16 collection. Some contained information about Canadians that went beyond that necessary for the understanding and exploitation of the intelligence. Although these represented only a very small fraction of the total, the Committee believes that the Service could be more circumspect with little or no penalty to the quality of its analyses.

The Committee recommends that CSIS ensure that it is more circumspect and that reports to requesting agencies contain only that information absolutely essential for the exploitation of the foreign intelligence.

Finally, the Committee was encouraged to observe that the incidental interception of information about Canadian businesses was minimal. The Members also found that the use made of section 16

information in certain types of ongoing section 12 (national security) investigations was insignificant. However, the Committee is alert to the possibility that this situation could change if, as we anticipate, the Service were to focus its section 12 investigations in new directions.

Management, Retention and Disposal of Files

Files are the essential currency of intelligence gathering. Each CSIS investigation and every approved target requires the creation of a file and a system for making the information in it available to those designated within the Service. Balanced against this information-gathering apparatus is the clear restriction on CSIS set out in the CSIS Act, that it shall collect information “to the extent that it is strictly necessary.” The Committee closely monitors annually the operational files held by the Service.

FILE DISPOSAL

CSIS files are held according to predetermined retention and disposal schedules that are negotiated with the National Archivist. These define how long the files are to be retained after Service employees cease using them. When this period expires, the National Archives Requirements Unit (NARU) in CSIS consults with Service operations staff on whether to keep the file, destroy it or send it to the National Archives.

During fiscal year 1999–2000, NARU reviewed 44 223 files, which had come to their attention through the regular archival “Bring Forward” (BF) system. Most of the files reviewed by NARU were from the screening and administration sections of the Service.

Of the files that NARU and the operational staff reviewed, 33 920 were destroyed and 10 097 were

retained. CSIS informed us that 206 files were identified as having archival value. They were removed from the active file holdings and automated systems and will be sent to National Archives at a future date, according to the established schedules.

Overlooked Files—Follow Up

Last year the Committee reported on certain files that had been overlooked by the Service's file management system. The committee asked that CSIS reassess the files for their operational value and dispose of them appropriately.

The Committee has since been informed by the Service that of the sample we examined, all were either destroyed or transferred to the National Archives. Of the total files remaining in the overlooked category, approximately one-third have been retained because they contain information of operational value and the balance destroyed or sent to the National Archives.

Security Screening and Investigation of Complaints

The Committee's enabling legislation—the *CSIS Act*—gives it a dual mandate: to review all CSIS activities and to investigate any complaints made about its activities. This section of the report deals with the second of the Committee's main responsibilities.

A. Security Screening

The Service has the authority, under section 15 of the *CSIS Act*, to conduct investigations in order to provide security assessments to departments and agencies of the Federal and provincial governments (section 13); the government of a foreign state (section 13); and the Minister of Citizenship and Immigration (section 14).

For Federal employment, CSIS security assessments serve as the basis for determining an individual's suitability for access to classified information or assets. In immigration cases, Service assessments can be instrumental in Citizenship and Immigration Canada's decision to admit an individual into the country and in the granting of permanent resident status or citizenship.

SECURITY SCREENING FOR FEDERAL EMPLOYMENT

1999–2000 Key Statistics

- The number of security screening assessments rendered under the Government Security Program for Level I, II and III clearances totaled 33 357, with an average turnaround time of 8 days for a Level I assessment, 9 days for Level II and 72 days for Level III.
- The greatest number of the 4599 field investigations was required by the Department of National Defence, followed by Foreign Affairs and

International Trade, CSIS, Public Works and Government Services, Communications Security Establishment, Privy Council Office and Citizenship and Immigration Canada.

- The Service also gave 25 160 assessments for the Airport Restricted Access Area Clearance Program (ARAACP), which is under the authority of Transport Canada. The average turnaround time for an ARAACP request was 4 days.
- Of the 58 517 assessments rendered in total, the Service issued 12 government briefs. Three recommended denial of a clearance and 9 were “information briefs.”
- The three government denial briefs were all in relation to Level II clearances in three separate Federal Government departments. Two of the individuals concerned exercised their right of review by lodging a complaint before the Committee pursuant to section 42 of the *CSIS Act*.

New Security Screening Procedures for the “Parliamentary Precinct”

Under the Government Security Policy (GSP), CSIS is responsible for conducting security screening investigations for all Federal Government departments except the RCMP. Prior to 1998, Parliament—not being a government department—relied on the RCMP to provide criminal records checks as there were no CSIS records checks done for employees of Parliament. On the basis of public safety, checks for Parliamentary employees are now conducted under the Security Accreditation Checks Program. On March 1, 2000, the Service commenced security records checks for prospective employees of the Senate and independent contractors working for the Senate.

With the RCMP acting as intermediary, Parliamentary employees are subject to the Security Accreditation Checks Program procedures. Security accreditations granted under the new procedures are valid for five

years and are not transferable to other government departments.

The Committee was concerned to learn that, as with airport employees subject to the Airport Restricted Access Area Clearance Program (ARAACP), employees of the new Parliamentary Precinct will not have the right to bring a complaint about security screening to the Review Committee. The Committee has repeatedly stated its view that all persons—regardless of employment status—subject to the potential impact of adverse information collected by CSIS during security screening investigations should have access to redress through the Review Committee.

IMMIGRATION SECURITY SCREENING PROGRAMS

Under the authority of sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to the Minister of Citizenship and Immigration Canada (CIC). Generally speaking, the Service's assistance 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 the form of "assessments" with respect to the inadmissibility classes of section 19 of the *Immigration Act*.

Applications for Permanent Residence from Within Canada

The Service has the sole responsibility for screening immigrants and refugees who apply for permanent residence status from within Canada. In 1999–2000, the Service received 52 742 requests²¹ for screening applicants under this program. The average turn-around time for screenings was 21 days—18 days for electronic applications and 94 days for paper applications.

Applications for Permanent Residence from Outside Canada

Immigration and refugee applications for permanent residence that originate outside of Canada are managed by the Overseas Immigrant Screening Program.

Under this program, CSIS shares the responsibility for security screening with CIC officials abroad. As a general rule, CSIS only becomes involved in the screening process if requested to do so by the Immigration Program Manager (IPM) or upon receipt of adverse information about a case from established sources—an arrangement that allows the Service to concentrate on higher risk cases.

In 1999–2000, the Service received 24 493 requests to screen offshore applicants and 4415 applicant files were referred to CSIS Security Liaison Officers (SLO) for consultation.

Citizenship Applications and the Alert List

As part of the citizenship application process the Service receives electronic trace requests from CIC's Case Processing Centre in Sydney, Nova Scotia. The names of citizenship applicants are cross-checked against the names in the Security Screening Information System database. The Service maintains an Alert List comprised of individuals who have come to the attention of CSIS through TARC-approved investigations and who have received landed immigrant status.

In 1999–2000 the Service received 192 717 trace requests from CIC. Of those requests, 34 resulted in information briefs, none of which included advice recommending the denial of citizenship. In two cases the Service requested a deferral of its advice.²²

Nature of the Service's Advice to CIC

Of the 81 650²³ immigration security screening assessments conducted by CSIS during the year under review, the Service forwarded briefs on 166 to CIC. Fifty-seven were information briefs containing security-related information but stopping short of a finding of inadmissibility. The other 109 contained Service notification that it had information that the applicant "is or was" a member of an inadmissible class of persons as defined in section 19(1) of the *Immigration Act*.²⁴

Committee's Upcoming Review of CSIS Security Screening Briefs

In the upcoming year, the Committee intends to conduct a full review of CSIS security screening briefs to Government both for Federal employees and for investigations conducted for the immigration program. We will report our findings in the 2000–2001 annual report.

SCREENING ON BEHALF OF FOREIGN AGENCIES

The Service may enter into reciprocal arrangements with foreign agencies to provide security checks on Canadians and other individuals who have resided in Canada. In 1999–2000 the Service concluded 876 foreign screening checks, 124 of which required field investigations. These investigations resulted in two information briefs.

B. Investigations of Complaints

Besides the Committee's function to audit and review the Service's intelligence activities, we have the added task of investigating complaints from the public

about any CSIS action. Three areas fall within the Committee's purview:

- As a quasi-judicial tribunal the Committee is empowered to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees and contractors.
- The Committee can investigate reports made by Government Ministers about persons in relation to citizenship and immigration, certain human rights matters and organized crime.
- As stipulated in the *CSIS Act*, the Committee can receive at any time a complaint lodged by a person "with respect to any act or thing done by the Service."

FINDINGS ON SECTION 41 COMPLAINTS—“ANY ACT OR THING”

During the 1999–2000 fiscal year, the Committee dealt with 67 complaints under section 41 of the *CSIS Act* (“any act or thing”). Forty-eight of these were new complaints and 19 cases were continued from the previous fiscal year (*see* Table 2).

Table 2
Complaints (April 1, 1999 to March 31, 2000)

	New Complaints	Carried Over from 1998–1999	Closed in 1999–2000	Carried forward to 1999–2000
CSIS Activities	48	19	50	17
Security Clearances	4	1	1	4
Immigration	1	0	0	1
Citizenship	1	0	0	1
Human Rights	1	0	0	1

Immigration-Related Complaints

The year under review again confirmed a trend toward increased numbers of complaints filed in relation to CSIS activities in immigration security screening. Of the 67 complaint cases handled by the Committee in 1999–2000, 32 dealt with immigration matters. Three of the complaints resulting in reports are summarized in Appendix D, “Complaint Case Histories.”

Complaints Concerning Improper Conduct and Abuse of Power

Nineteen of the section 41 complaints handled in 1999–2000 concerned individuals alleging that the Service had subjected them to surveillance, illegal actions or had otherwise abused its powers. In the majority of these the Committee concluded after investigating that the Service was neither involved in nor responsible for the activities being alleged.

In one instance, however, we believe the Service demonstrated poor judgment in disclosing information to a complainant in light of the knowledge the Service had about the individual and the possible impact of such disclosure on the complainant’s well-being. In two other cases, the Committee was able to assure complainants that the Service had not passed information about them to third parties.

So as not to confirm indirectly which targets are of interest to the Service, the Committee does not, as a rule, confirm one way or another to a complainant whether he or she is the subject of a CSIS targeting authority. The Committee does, however, conduct a thorough investigation into the complainant’s allegations.

If the individual has in fact been a Service target, the Committee assures itself that the targeting has been carried out in accordance with the *Act*, Ministerial Direction and CSIS policy. If we find that the Service has acted appropriately we convey that assurance to the complainant. If we find issues of concern we share

those with the Director of CSIS and the Solicitor General, and to the extent possible, report on the matter in our annual report.

Complaints the Committee was Precluded from Investigating

The Committee was precluded from investigating some cases because criteria set out in section 41 of the *Act* had not been met. In these cases the complainant had not first made the complaint to the Director of CSIS or the individuals concerned were entitled to seek redress through other means set out in the *Public Service Staff Relations Act* and the *CSIS Act*. In all cases, the complainants were notified of the Committee’s decision.

Misdirected Complaints

The Committee received a small number of complaints that involved neither CSIS nor issues of national security. To the extent possible, and after having informed the individual that the complaint was not within the Committee’s jurisdiction, we attempted to redirect the complaints to the appropriate authorities.

FINDINGS ON SECTION 42 COMPLAINTS— “DENIAL OF A SECURITY CLEARANCE”

In 1999–2000, the Committee investigated five complaints arising from denials of security clearances. Two concerned the revocation of existing clearances; three others related to the denial of new clearances. A case for which a Committee report has been issued is summarized in Appendix D; the investigation for another case was completed and the report is pending. Three others have been carried over into next year.

FINDINGS ON MINISTERIAL REPORTS

Citizenship Refusals

In the ongoing matter of the citizenship application of Ernst Zündel, in June 1999, Justice McKeown of

the Federal Court rejected Mr. Zündel's application for a review of an earlier ruling. This decision was appealed, and the Court dismissed the appeal with costs.

In its ruling, the Bench of the Federal Court of Appeal²⁵ was of the view that the appeal could not succeed. If the Court assumed that it was, in effect, the earlier Ministerial Report that was under review, the time limit for such review had expired. If, on the other hand, the Court were to assume that it was the Committee's letter of March 31, 1999 that was at issue, the Court could discern no error in the letter that would warrant the Court's intervention. In sum, it was the Court's view that the Minister's Report was sufficient to initiate an investigation by the Committee, that the Report obligated the Committee to investigate and that the Committee had the legal mandate to do so.

As a consequence of this decision, the Committee Member presiding over the case refused to grant a stay of proceedings to allow Mr. Zündel to obtain leave from the Supreme Court to further appeal the ruling of the Federal Court of Appeal. The matter is scheduled to resume in late 2000.

Reports Pursuant to the Immigration Act

The Committee received no Ministerial Reports of this type during the year under review. However, a case involving a report received in 1996–97 has once again been referred to the Committee.

In a decision rendered on March 14, 2000, Justice Gibson of the Federal Court Trial Division quashed a SIRC 1998 report, which found that a subject of an earlier Ministerial Report did in fact fall under the class of inadmissible persons described in the *Immigration Act*. (see inset *Yamani v. Canada* for more details on the ruling.)

Following Justice Gibson's decision, the matter was referred back to the Committee to be redetermined in accordance with the law, the Federal Court decision and the two judicial reviews. Before rehearing and redetermining the matter the Committee will seek confirmation from the Minister of Citizenship and Immigration Canada that CIC intends to pursue the matter.

CANADIAN HUMAN RIGHTS COMMISSION REFERRALS

During the year under review the Committee received no Human Rights Commission referrals. We did complete an investigation from the previous year involving a group of current and ex-employees of CSIS. The Committee will report its findings to the Commission shortly. The Committee noted that the Service granted a security clearance to complainants' counsel so that complainants could fully discuss the nature of their work while ensuring that sensitive information remained properly protected.

Yamani v. Canada (Minister of Citizenship and Immigration) 2000 F.C.J. No.317

This case involved judicial review of a report issued by the Committee to the Governor in Council in April 1998 pursuant to section 39 of the *Immigration Act*.²⁶ In the report, the Committee found that a certificate under section 40(1) of the *Immigration Act*—possibly leading to the forfeiture of the right to remain in Canada—should be issued in respect of Mr. Yamani as he was a person described in sections 19(1)(e) and 19(1)(g) of the *Immigration Act*.

This report was the second issued by the Committee about Mr. Yamani. The first was set aside by order of Mr. Justice MacKay in 1996 and referred back to the Committee.²⁷

In the review of the Committee's most recent report the court considered the following:

- Whether the Committee erred in law by finding it lacked the jurisdiction to consider and rule on constitutional challenges to the validity of the legislation it is required to apply.
- Whether the terms “subversion,” “democratic government, institutions and processes” and “reasonable grounds to believe” found in section 19 of the *Immigration Act* were invalid as they violated Mr. Yamani's constitutional rights and should therefore be found to be of no force and effect.²⁸
- Whether the Committee had erred in law by ignoring or misinterpreting evidence and whether such errors led to unreasonable conclusions by the Committee.

The first of these three issues was not pursued because the constitutional challenges were argued *de novo* in the context of the second issue. With respect to the second issue, Mr. Justice Gibson upheld the challenged provisions as valid under the *Charter*.²⁹

On the third issue, Mr. Justice Gibson concluded that the evidence about the current and future capacity of the organization to which the complainant belonged—the Popular Front for the Liberation of Palestine (PFLP)—showed that it was not the potent, radical terrorist organization it once was. Justice Gibson held that the Committee appeared to have ignored the testimony of an expert witness to the effect that subversion has two essential characteristics. First that it be clandestine or deceptive, and second, that it involve undermining from within. Under this definition, Mr. Justice Gibson concluded, Mr. Yamani could not be said to have engaged in subversion against the state of Israel, either directly or through support of or membership in the PFLP, because being external to the state of Israel, the organization could not undermine from within. Consequently, Mr. Justice Gibson found that the Committee had erred in law in relying “without further analysis” on the definition of “subversion” given in the *Shandi* case³⁰ and in concluding that Mr. Yamani was a person described in section 19(1)(e) of the *Immigration Act*.

With respect to the Committee's finding that Mr. Yamani was a person described under section 19(1)(g) of the *Immigration Act*, Mr. Justice Gibson found the Committee's analysis insufficient to support its conclusion. The court thus could not allow the Committee's finding to stand. In SIRC's favour, however, the court did find that the Committee's concerns about Mr. Yamani's credibility were justified.³¹

Justice Gibson ordered that the matter be remitted to the Committee for reconsideration.

CSIS Accountability Structure

The Service is an agency of the Government of Canada which reports to the Solicitor General who in turn is accountable to Parliament. Because of the serious and potentially intrusive nature of CSIS activities, the mechanisms set out in law to give effect to that accountability are both rigorous and multi-dimensional; a number of independently managed systems exist inside and outside the Service for monitoring CSIS activities and ensuring that they accord with its mandate.

Part of SIRC's task (the Committee itself being part of the accountability structure) is to assess and comment on the functioning of the systems that hold the Service responsible to government and Parliament.

A. Operation of CSIS Accountability Mechanisms

MINISTERIAL DIRECTION

Under section 6(2) of the *CSIS Act*, the Minister can issue directions governing CSIS investigations. Also according to the *Act*, the Committee is specifically charged with reviewing directions issued by the Minister. We assess new directions when they are released by the Minister and examine how the Direction is applied in specific, actual cases.

National Requirements for Security Intelligence 1999–2000 and 2000–2001

National Requirements contain general direction from Cabinet as to where CSIS should focus its investigative efforts, as well as guidance on the Service's collection, analysis, and advisory responsibilities. The Committee received the 1999–2000 National Requirements in August 1999 and so was not able to report on them in last year's Annual Report. The 2000–2001 Requirements were received in a timely manner so both are addressed here.

Both sets of Requirements varied little from those of 1998–1999, reflecting a relatively unchanged threat environment. Changes that drew the Committee's attention were as follows:

- the list of groups identified as threats to national security under investigation by the Counter Terrorism Program was altered slightly;
- in addition to the mention of specific threats, transnational criminal activity is now more generally regarded as a threat to Canada's economic security and the integrity of government programs;
- CSIS was directed to increase its research and development efforts so as to keep pace with technological innovations and maintain its investigative capacities. CSIS was provided with 70 percent of the requested funding for this initiative.

CHANGES IN SERVICE OPERATIONAL POLICIES AND INSTRUCTIONS TO OFFICERS

No new policies were issued in the fiscal year under review. Existing policies amended in a material way addressed the following areas:

- Ministerial approval procedures for source operations in a sensitive institution;
- conflict of interest guidelines for human sources;
- the level of detail required in operational plans;
- information and intelligence disclosure caveats to reflect changes in the *Canada Evidence Act*.

DISCLOSURES OF INFORMATION IN THE PUBLIC AND IN THE NATIONAL INTEREST

Section 19 of the *CSIS Act* prohibits disclosure of information obtained by the Service in the course of its investigations, except in specific circumstances. Under section 19(2)(d), however, the Minister can

authorize the Service to disclose information in the “public interest.” The *Act* compels the Director of CSIS to submit a report to the Committee regarding all “public interest” disclosures. There were no such reports in 1999–2000.

In addition, CSIS can—in the role as the Minister’s agent—disclose information in special circumstances in the “national interest.” Service policy stipulates that the Committee must be so informed. There were no such disclosures during the year under review.

GOVERNOR IN COUNCIL REGULATIONS AND APPOINTMENTS

As set out in section 8(4) of the *CSIS Act*, the Governor in Council may issue any regulations to the Service in regard to the powers and duties of the Director of CSIS, and/or the conduct and discipline of Service employees. No regulations were issued by the Governor in Council in fiscal year 1999–2000.

CERTIFICATE OF THE INSPECTOR GENERAL

The Inspector General of CSIS reports to the Solicitor General and functions effectively as his internal auditor of 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 Director’s report on the operational activities of the Service and informing the Minister of any instances of CSIS having failed to comply with the *Act* or Ministerial Direction, or that involved an unreasonable or unnecessary exercise of powers. The Minister also forwards the Certificate to the Review Committee.

Between June 1998 and September 1999, the position of Inspector General of CSIS was vacant. As a result, no Certificate was issued by that office for fiscal year 1998–1999. On July 29, 1999, the Solicitor General of Canada announced the appointment of Maurice Archdeacon as the new Inspector General. Mr.

Archdeacon had been SIRC’s Executive Director since its establishment in 1985.

The Committee was informed that the Inspector General’s Certificate for 1999–2000 would be sent to the Solicitor General of Canada in Autumn 2000—too late for review in this report. We will comment on the new Inspector General’s first Certificate next year.

UNLAWFUL CONDUCT

Under section 20(2) of the *CSIS Act*, the Director of CSIS is to submit a report to the Minister when, in his opinion, a CSIS employee may have acted unlawfully in the performance of his or her duties and functions. The Minister, in turn, must send the report with his comment to the Attorney General of Canada and to the Committee.

In 1999–2000, no cases of unlawful conduct were brought to the Minister’s attention.

In last year’s report, the Committee commented on one report of possible unlawful conduct by an employee of CSIS. We learned that no decision had been taken by the Attorney General of Canada concerning this case.

We also commented on another case of unlawful conduct dating back to 1997 that was still pending. We have since been informed that both the criminal investigation and the Service’s internal inquiry into this matter have been concluded. The Service advised the Minister that it was unable to establish that the employee in question acted unlawfully in the performance of his or her duties and that following the criminal investigation, the Crown Attorney elected not to lay charges. In this matter, the Attorney General of Canada has yet to render a decision.

CSIS ANNUAL OPERATIONAL REPORT

The CSIS Director’s Annual Operational Report to the Solicitor General comments in some detail on the Service’s operational activities for the preceding fiscal

year. Among the functions of the Committee is to review this report.

Last year, the Committee did not receive the Service report in time for inclusion in our 1998–99 audit report. Therefore, we present that review here, as well as our comments on the 1999–2000 Director’s report.

Annual Operational Report for 1998–99

As in previous years, the 1998–99 CSIS Annual Operational Report contained extensive updates on CSIS investigations. However, this particular report was a departure from past practice in that it also addressed some strategic issues as well—notably a discussion of the technological challenges facing the Service. The Committee, in past reviews, had urged the Director to make greater efforts to provide commentary on significant global trends and policy issues with potential impact on Canadian security intelligence activities.

Annual Operational Report for 1999–2000

The Committee is particularly interested in the use made by Director of CSIS of the authority delegated to him by the Minister. Existing Ministerial Direction requires the Director to provide summaries of cases where delegated authority was in fact used.

In reviewing the 1999–2000 document, it appeared to the Committee that the manner in which the Director reported on these cases varied considerably. For instance, with respect to the use of human sources, the report provided summaries of each case. However, in other areas of Service activity—inter-agency co-operation, for example—the report discusses only the number of instances but omits further explanation.

In recent years, there have been clear improvements in the Annual Operational Report to the Minister. The Committee hopes that, in future, the report will be more consistent in providing descriptive summaries of the cases in which the Director has used powers delegated by the Minister.

SIRC INQUIRIES OF CSIS

Tracking and Timing of Formal Inquiries

In our review function we send questions to CSIS to request information or documents (or both) about its activities. In the 1999–2000 fiscal year (April 1, 1999 to March 31, 2000) we directed 107 formal inquiries to the Service, a slight decrease from last year. This figure does not include questions arising out of complaint cases.

In addition to formal questions, the Committee makes informal requests of CSIS. In all such cases for the year under review, the Service responded expeditiously to what were sometimes urgent queries.

Briefings

At its monthly meetings, the Chair and Committee Members meet with government officials to keep the lines of communication open and stay abreast of new developments. When meetings of the Committee are held outside of Ottawa, Members visit CSIS regional offices. The Committee met with senior CSIS regional managers in Montreal in September 1999 and Vancouver in May 2000. The balance of the Committee’s meetings were held in Ottawa.

B. Inside the Security Intelligence Review Committee

SIRC CHAIR REAPPOINTED

In June 2000, the Governor in Council reappointed the Honourable Paule Gauthier, P.C., O.C., Q.C., as Chair of the Committee for a five-year term.

NEW EXECUTIVE DIRECTOR APPOINTED

On November 1, 1999 the Honourable Paule Gauthier announced the appointment of Ms. Susan Pollak as the Executive Director of SIRC effective November 15, 1999.

Ms. Pollak began her public service career at the Communications Security Establishment (CSE) in 1973. Ms. Pollak was seconded to the Privy Council Office in 1984, and three years later, she accepted a position as principal advisor to the Deputy Clerk (Security and Intelligence, and Counsel). Since then, Ms. Pollak has held several senior management positions with the Treasury Board Secretariat, the Department of Fisheries and Oceans, and Natural Resources Canada.

ACTIVITIES ADDITIONAL TO CSIS REVIEW

- The Chair met with members of the House of Commons Standing Committee on Justice and Human Rights in February and March 2000 to discuss the role and functions of the Security Intelligence Review Committee and how SIRC can assist parliamentarians.
- A delegation from the United States General Accounting Office, a body of the US Congress, met with Committee Members in August 1999 to discuss a Congressional study of how other countries deal with terrorism.
- The Vice-President of France's Assemblée Nationale met with SIRC's Chair in September 1999 to discuss France's proposal to establish a parliamentary review body for intelligence matters.
- In October 1999 and again in January 2000, Members met with Canada's Minister of Citizenship and Immigration. The Committee also met with the Director of CSIS on two occasions: October 1999 and March 2000. In February 2000, the Committee met with the Deputy Secretary to the Cabinet, Security and Intelligence, who discussed her mandate in the Privy Council Office and current issues.
- In September 1999, Members accepted a long-standing invitation to meet with the Special Services Committee of Poland's Sejm (parliament). The purpose of the visit was to exchange information about the review process in new democracies. The Committee also travelled to the Czech Republic to meet with SIRC's counterpart there and with senior officials of that country's intelligence services.
- At the invitation of the Parliament of South Africa's Joint Standing Committee on Intelligence (JSCI), Committee Members travelled to South Africa to meet with JSCI members, the Minister of Intelligence Services, the Inspector General and senior intelligence service officials.

Table 3
SIRC Expenditures

	2000–2001 (Estimates)	1999–2000 (Actual)	1998–1999 (Actual)
Personnel	1 089 000	841 945	715 036
Goods and Services	962 000	821 055	656 730
Total	2 051 000	1 663 000	1 371 766

- In June 2000, the Committee's Counsel, Sylvia Mackenzie, participated in a Vancouver conference sponsored by the Canadian Council for Refugees.

ON THE INTERNET

All SIRC Annual Reports, dating back to 1984–85 when the Committee was created, are now accessible through our Web site (www.sirc-csars.gc.ca). The site offers information ranging from biographical information on the members of the Committee, to a list of Committee studies that is updated regularly. A “What’s New” hot link provides updates on SIRC activities, and other pages link readers to more sites of interest. In addition, the SIRC Web site describes procedures for filing complaints about CSIS activities and the denial of security clearances, as set out in sections 41 and 42 of the *CSIS Act*.

BUDGET AND EXPENDITURES

For 15 years the Committee has managed its activities within the resource levels established in 1985. In 1999–2000, the Committee experienced a significant increase in the number of quasi-judicial (complaints) proceedings with a concomitant impact on non-discretionary expenses (*see* Table 3).

Other major items of expense include:

- planned upgrades to the security-certified computer infrastructure—costly technology needed to support the Committee's functions and to meet the stringent security requirements for handling highly classified information;
- Committee Members' travel expenditures within Canada and for travel abroad at the invitation of other countries wishing to benefit from Canada's experience in review activities;
- staff salaries and benefits—for the first time since 1997, the Committee has had its full complement of researchers and Committee Members.

STAFFING AND ORGANIZATION

The Committee has a staff of 15: an executive director, a counsel/senior complaints officer to handle complaints and ministerial reports, two complaints officers (one of whom is the Committee registrar for hearings), a deputy executive director, a research manager, a senior policy advisor, a senior analyst/media liaison officer, three senior research analysts, a financial/office administrator, and an administrative support staff of three to handle sensitive and highly-classified material using special security procedures.

At its monthly meetings, the Members of the Committee decide formally on the research and other activities they wish to pursue and set priorities for the staff. Managing the day-to-day operations is delegated to the Executive Director with direction when necessary from the Chair in her role as the Chief Executive Officer of the organization.

Appendix A

Glossary

Glossary

ARAACP	Airport Restricted Access Area Clearance Program
BF	Bring Forward system
CI	Counter Intelligence
CIA	Central Intelligence Agency (United States)
CIC	Citizenship and Immigration Canada
Committee	Security Intelligence Review Committee (SIRC)
CSE	Communications Security Establishment (DND)
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism
DFAIT	Department of Foreign Affairs and International Trade
Director	The Director of CSIS
DND	Department of National Defence
EXIPC	Executive Intelligence Production Committee
GSP	Government Security Policy
IAC	Intelligence Assessment Committee (Privy Council Office)
IPM	Immigration Program Manager (CIC)
IWG	Interdepartmental Working Group
JSCI	Joint Standing Committee on Intelligence
MOU	Memorandum of Understanding
NARU	National Archives Requirements Unit (CSIS)

OIC	Officer in Charge (RCMP)
PFLP	Popular Front for the Liberation of Palestine
RAP	Requirements, Analysis & Production Branch (CSIS)
RCMP	Royal Canadian Mounted Police
RTA	Request for Targeting Authority
Service	Canadian Security Intelligence Service (CSIS)
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officers
TARC	Target Approval and Review Committee
WMD	Weapons of Mass Destruction

Appendix B

SIRC Reports and Studies Since 1984

SIRC Reports and Studies Since 1984

(Section 54 reports—special reports the Committee makes to the Minister—are indicated with an *)

1. *Eighteen Months After Separation: An Assessment of CSIS' Approach to Staffing Training and Related Issues*, (SECRET) * (86/87-01)
2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service*, (SECRET) * (86/87-02)
3. *The Security and Intelligence Network in the Government of Canada: A Description*, (SECRET) * (86/87-03)
4. *Ottawa Airport Security Alert*, (SECRET) * (86/87-05)
5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions*, (SECRET) * (87/88-01)
6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS*, (UNCLASSIFIED) * (86/87-04)
7. *Counter-Subversion: SIRC Staff Report*, (SECRET) (87/88-02)
8. *SIRC Report on Immigration Screening*, (SECRET) * (87/88-03)
9. *Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement*, (PUBLIC VERSION) * (87/88-04)
10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process*, (SECRET) * (88/89-01)
11. *SIRC Review of the Counter-Terrorism Program in the CSIS*, (TOP SECRET) * (88/89-02)
12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS*, (SECRET) * (89/90-02)
13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement*, (SECRET) * (89/90-03)
14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information*, (SECRET) (89/90-04)
15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information*, (SECRET) * (89/90-05)
16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons*, (UNCLASSIFIED) (89/90-06)
17. *SIRC Report on the Innu Interview and the Native Extremism Investigation*, (SECRET) * (89/90-07)
18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988*, (SECRET) * (89/90-01)
19. *A Review of the Counter-Intelligence Program in the CSIS*, (TOP SECRET) * (89/90-08)
20. *Domestic Exchanges of Information*, (SECRET) * (90/91-03)

21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue*, (SECRET) (90/91-06)
22. *Regional Studies (six studies relating to one region)*, (TOP SECRET) (90/91-04)
23. *Study of CSIS' Policy Branch*, (CONFIDENTIAL) (90/91-09)
24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets*, (TOP SECRET) (90/91-05)
25. *Release of Information to Foreign Agencies*, (TOP SECRET) * (90/91-02)
26. *CSIS Activities Regarding Native Canadians—A SIRC Review*, (SECRET) * (90/91-07)
27. *Security Investigations on University Campuses*, (TOP SECRET) * (90/91-01)
28. *Report on Multiple Targeting*, (SECRET) (90/91-08)
29. *Review of the Investigation of Bull, Space Research Corporation and Iraq*, (SECRET) (91/92-01)
30. *Report on Al Mashat's Immigration to Canada*, (SECRET) * (91/92-02)
31. *East Bloc Investigations*, (TOP SECRET) (91/92-08)
32. *Review of CSIS Activities Regarding Sensitive Institutions*, (TOP SECRET) (91/92-10)
33. *CSIS and the Association for New Canadians*, (SECRET) (91/92-03)
34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) * (91/92-04)
35. *Victor Ostrovsky*, (TOP SECRET) (91/92-05)
36. *Report on Two Iraqis—Ministerial Certificate Case*, (SECRET) (91/92-06)
37. *Threat Assessments, Section 40 Study*, (SECRET) * (91/92-07)
38. *The Attack on the Iranian Embassy in Ottawa*, (TOP SECRET) * (92/93-01)
39. *"STUDYNT" The Second CSIS Internal Security Case*, (TOP SECRET) (91/92-15)
40. *Domestic Terrorism Targets—A SIRC Review*, (TOP SECRET) * (90/91-13)
41. *CSIS Activities with respect to Citizenship Security Screening*, (SECRET) (91/92-12)
42. *The Audit of Section 16 Investigations*, (TOP SECRET) (91/92-18)
43. *CSIS Activities during the Gulf War: Community Interviews*, (SECRET) (90/91-12)
44. *Review of CSIS Investigation of a Latin American Illegal*, (TOP SECRET) * (90/91-10)
45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review*, (TOP SECRET) * (91/92-14)
46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)*, (TOP SECRET) * (90/91-11)
47. *The Assault on Dr. Hassan Al-Turabi*, (SECRET) (92/93-07)

48. *Domestic Exchanges of Information (A SIRC Review—1991/92)*, (SECRET) (91/92-16)
49. *Prairie Region Audit*, (TOP SECRET) (90/91-11)
50. *Sheik Rahman's Alleged Visit to Ottawa*, (SECRET) (CT 93-06)
51. *Regional Audit*, (TOP SECRET)
52. *A SIRC Review of CSIS' SLO Posts (London & Paris)*, (SECRET) (91/92-11)
53. *The Asian Homeland Conflict*, (SECRET) (CT 93-03)
54. *Intelligence-Source Confidentiality*, (TOP SECRET) (CI 93-03)
55. *Domestic Investigations (1)*, (SECRET) (CT 93-02)
56. *Domestic Investigations (2)*, (TOP SECRET) (CT 93-04)
57. *Middle East Movements*, (SECRET) (CT 93-01)
58. *A Review of CSIS' SLO Posts (1992-93)*, (SECRET) (CT 93-05)
59. *Review of Traditional CI Threats*, (TOP SECRET) (CI 93-01)
60. *Protecting Science, Technology and Economic Interests*, (SECRET) (CI 93-04)
61. *Domestic Exchanges of Information*, (SECRET) (CI 93-05)
62. *Foreign Intelligence Service for Canada*, (SECRET) (CI 93-06)
63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 93-11)
64. *Sources in Government*, (TOP SECRET) (CI 93-09)
65. *Regional Audit*, (TOP SECRET) (CI 93-02)
66. *The Proliferation Threat*, (SECRET) (CT 93-07)
67. *The Heritage Front Affair. Report to the Solicitor General of Canada*, (SECRET) * (CT 94-02)
68. *A Review of CSIS' SLO Posts (1993-94)*, (SECRET) (CT 93-09)
69. *Domestic Exchanges of Information (A SIRC Review 1993-94)*, (SECRET) (CI 93-08)
70. *The Proliferation Threat—Case Examination*, (SECRET) (CT 94-04)
71. *Community Interviews*, (SECRET) (CT 93-11)
72. *An Ongoing Counter-Intelligence Investigation*, (TOP SECRET) * (CI 93-07)
73. *Potential for Political Violence in a Region*, (SECRET) (CT 93-10)
74. *A SIRC Review of CSIS' SLO Posts (1994-95)*, (SECRET) (CT 95-01)
75. *Regional Audit*, (TOP SECRET) (CI 93-10)
76. *Terrorism and a Foreign Government*, (TOP SECRET) (CT 94-03)
77. *Visit of Boutros Boutros-Ghali to Canada*, (SECRET) (CI 94-04)

78. *Review of Certain Foreign Intelligence Services*, (TOP SECRET) (CI 94-02)
79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 94-01)
80. *Domestic Exchanges of Information (A SIRC Review 1994–95)*, (SECRET) (CI 94-03)
81. *Alleged Interference in a Trial*, (SECRET) (CT 95-04)
82. *CSIS and a “Walk-In”*, (TOP SECRET) (CI 95-04)
83. *A Review of a CSIS Investigation Relating to a Foreign State*, (TOP SECRET) (CI 95-02)
84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TOP SECRET) (CI 95-05)
85. *Regional Audit*, (TOP SECRET) (CT 95-02)
86. *A Review of Investigations of Emerging Threats*, (TOP SECRET) (CI 95-03)
87. *Domestic Exchanges of Information*, (SECRET) (CI 95-01)
88. *Homeland Conflict*, (TOP SECRET) (CT 96-01)
89. *Regional Audit*, (TOP SECRET) (CI 96-01)
90. *The Management of Human Sources*, (TOP SECRET) (CI 96-03)
91. *Economic Espionage I*, (SECRET) (CI 96-02)
92. *Economic Espionage II*, (TOP SECRET) (CI 96-02)
93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97*, (TOP SECRET) (CI 96-04)
94. *Urban Political Violence*, (SECRET) (SIRC 1997-01)
95. *Domestic Exchanges of Information (1996–97)*, (SECRET) (SIRC 1997-02)
96. *Foreign Conflict, Part I*, (SECRET) (SIRC 1997-03)
97. *Regional Audit*, (TOP SECRET) (SIRC 1997-04)
98. *CSIS Liaison with Foreign Agencies*, (TOP SECRET) (SIRC 1997-05)
99. *Spy Case*, (TOP SECRET) (SIRC 1998-02)
100. *Domestic Investigations (3)*, (TOP SECRET) (SIRC 1998-03)
101. *CSIS Cooperation with the RCMP, Part I*, (SECRET) * (SIRC 1998-04)
102. *Source Review*, (TOP SECRET) (SIRC 1998-05)
103. *Interagency Cooperation Case*, (TOP SECRET) (SIRC 1998-06)
104. *A Case of Historical Interest*, (TOP SECRET) (SIRC 1998-08)
105. *CSIS’ Role in Immigration Security Screening*, (SECRET) (CT 95-06)
106. *Foreign Conflict—Part II*, (TOP SECRET) (SIRC Study 1997-03)
107. *Review of Transnational Crime* (SECRET) (SIRC Study 1998-01)

108. *CSIS Cooperation with the RCMP—Part II* (SECRET) * (SIRC Study 1998-04)
109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98* (TOP SECRET) (SIRC Study 1998-07)
110. *Review of Intelligence Production* (SECRET) (SIRC Study 1998-09)
111. *Regional Audit* (TOP SECRET) (SIRC Study 1998-10)
112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC Study 1998-11)
113. *Allegations by a Former CSIS Employee*, (TOP SECRET) * (SIRC 1998-12)
114. *CSIS Investigations on University Campuses* (SECRET) (SIRC Study 1998-14)
115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC Study 1998-15)
116. *Files* (TOP SECRET) (SIRC Study 1998-16)
117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET) (SIRC Study 1999-01)
118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET) (SIRC Study 1999-02)
119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC Study 1999-03)
120. *Proliferation* (TOP SECRET) (SIRC Study 1999-04)
121. *Domestic Targets* (TOP SECRET) (SIRC Study 1999-06)
122. *Terrorist Fundraising* (TOP SECRET) (SIRC Study 1999-07)
123. *Regional Audit* (TOP SECRET) (SIRC Study 1999-08)
124. *Foreign State Activities* (TOP SECRET) (SIRC Study 1999-09)
125. *Project Sidewinder* (TOP SECRET) (SIRC Study 1999-10)
126. *Security Breach* (TOP SECRET) (SIRC Study 1999-11)

Appendix C

Recommendations and Major Findings

Project Sidewinder

The Committee found no evidence of political interference as alleged. None of the documents or records reviewed, interviews conducted or representations received evidenced such interference, actual or anticipated. Project Sidewinder was not terminated; it was delayed when its product was found to be inadequate.

With respect to the first Sidewinder draft report, we found the draft to be deeply flawed in almost all respects. The report did not meet the most elementary standards of professional and analytical rigour. The actions the Service took to ensure that subsequent products of its collaborative effort with the RCMP on Project Sidewinder would be of higher quality were appropriate.

The Committee found no evidence of any substantial and immediate threat of the sort envisaged in the first Sidewinder draft, no evidence that a threat was being ignored through negligence or design and no evidence that the Government had not been appropriately warned of substantive threats where such existed. Both CSIS and the RCMP continue to investigate similar threats separately.

The Committee found no indication that the disagreements between CSIS and the RCMP, which arose during the course of Project Sidewinder, had caused, or were symptomatic of, difficulties in other areas of the inter-agency relationship.

The Service disposed of what it regarded as “transitory documents” related to the Sidewinder first draft report. It is unable to locate other documents the Committee regards as clearly non-transitory and has stated that these were not disposed of but rather “misfiled.” However, the Committee does not believe this lapse had a material impact on the events surrounding Project Sidewinder; nor is there any evidence that raw information, kept in Service files and in part used by the Sidewinder analysts to compile their first report, was disposed of or altered in any manner.

Lost Documents—A Serious Breach of Security

On October 10, 1999, the vehicle of a CSIS Headquarters employee was vandalized in the Greater Toronto area. Inside the vehicle were a number of CSIS documents, several of which were classified. These were among the items stolen.

Following an investigation by the Service’s Internal Security Branch the employee was dismissed from the Service. In addition, the Service altered some of its procedures for document control and strengthened its internal “security awareness” program.

The Service’s own “lost documents” investigation was conducted in a competent and professional manner, ultimately revealing how its classified materials went astray. In the course of its investigation, Internal Security had considerable difficulty determining the precise content of one item, and thus had to make an educated guess at what the employee held at the time of the burglary. This apparent lapse helped nudge the Committee toward the conclusion that there may have been a problem in CSIS internal document control procedures generally.

We are aware that the Service periodically conducts its own internal review of security procedures. Nevertheless, security breaches in recent years involving CSIS materials suggests that these internal reviews have not been as effective as the Service and the Committee would have wished.

Threats from a Foreign Conflict

The threat perceived by the Service arose chiefly from the activities of foreign intelligence services operating in Canada. These included suspected attempts to raise funds, collect information on homeland communities, foment civil unrest in Canada and illegally procure weapons and technology.

The Committee determined that the Service had sufficient grounds to conduct the investigation and to employ the investigative methods permitted in the targeting authorities and Court warrants.

Three issues drew the Committee's attention:

- an overly general targeting authority giving rise to a formal recommendation:

The Committee recommends that RTAs be structured and written to identify clearly the reasons for targeting each target named, under each threat definition cited.
- an instance in which a CSIS officer made well-intentioned but inappropriate comments during the course of conducting an interview.
- an instance where information collected did not meet the “strictly necessary” test. The Service agreed with this finding and deleted the information from its database.

Terrorist Fundraising

The purpose of the Committee's study was to examine several facets of the Service's work in addressing the problems of terrorist fundraising in Canada. Our goals were twofold: to determine the effectiveness of Service advice in assisting the Government's efforts to curb terrorist fundraising and to ensure that all CSIS actions were appropriate and in conformity with the law.

The Service stated that, as a result of its investigations linked to international terrorism, it had uncovered several Canadian organizations suspected of facilitating terrorist fundraising objectives. Our own review of these investigations showed that CSIS did have sufficient information to believe that the links to international terrorist groups and to their fundraising efforts constituted a threat to the security of Canada.

CSIS and its departmental clients both expressed satisfaction with the liaison relationship. Recipients of Service reports said that the information had been most useful as “investigative leads” assisting in determining how and where to follow up.

Two recommendations emerged from this study. First, in respect of the nature of the Service's advice,

The Committee recommends that in future, CSIS advise its client departments of substantive changes to the assessments it has previously given them, which arise as a consequence of new information.

Second, although the Committee supports legislative changes that would allow more effective use to be made of the information shared between CSIS and its client departments, such enhanced procedures could well generate an increase in the number of complaints brought to the Committee. To address such an eventuality,

The Committee recommends that the Ministry of the Solicitor General and Privy Council Office initiate special measures to keep SIRC apprised, on a timely basis and as appropriate, of the IWG's (Interdepartmental Working Group on Countering Terrorist-Support Activities) proposals as they impact on CSIS activities.

Investigation of a Domestic Target

During a previous review, the Committee learned of several CSIS source operations that sometimes involved the legitimate dissent milieu—specifically, certain protests and demonstrations. We subsequently reviewed the investigations.

The Committee's review identified no violations of Service policy or Ministerial Direction. CSIS had reasonable grounds to suspect that the targets were threats to the security of Canada. Notwithstanding our general conclusions, this set of investigations was the source of some residual concerns for the Committee.

The Committee believes these point to an occasional lack of rigour in the Service's application of existing policies, which oblige it to weigh the requirement to protect civil liberties against the need to investigate potential threats. The Committee would like to see tangible evidence that significant investigatory decisions involving the legitimate dissent milieu are adequately weighed.

The Committee recommends that the Service make the changes to its administrative procedures necessary to ensure that all significant investigatory decisions in the area of lawful advocacy, protest and dissent are weighed and so documented.

The Committee believes that as well as providing an additional measure of comfort to the Review Committee, such changes would help maintain the day-to-day sensitivity of all CSIS staff to the need to protect civil liberties.

The Committee had an additional recommendation concerning the need to clarify a section of the CSIS *Operational Policy Manual* (a classified document).

A Long-Running Counter Intelligence Investigation

It is the Service's view that the target of this investigation is engaged in intelligence-related activities that manifest themselves in classical espionage, foreign influence in various aspects of Canadian society and the theft of economic and scientific information through clandestine means.

In an earlier report the Committee stated that “the threats posed by the intelligence gathering activities of this [target] [were] at th[e] time, nebulous, and sometimes hard to define.” Although events since then have served to confirm that the potential for serious threat to Canadian interests is serious and genuine, the current threat as measured in concrete and confirmed activity appears to us to be limited and infrequent.

This difference of opinion between CSIS and the Committee about the nature of the threat led us to conclusions about some of the target's activities that were at odds with those of the Service. Some of the activities investigated by the Service showed the target engaged in intelligence gathering in Canada, but others did not.

The Committee believes each of the targeting decisions examined was justified by the evidence. However, in the Service's application to secure warrant powers against one target were a number of overstatements.

The Committee believes that the potential threat to Canadians and Canadian interests arising from the activities of this target is significant. However, our review evidenced a few instances that pointed to the Service occasionally drawing conclusions not based on the facts at hand.

Domestic Exchanges of Information (4)

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. Under section 38(a)(iii) of the *Act*, the Committee is charged with the task of examining the co-operation arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

The Committee found that CSIS co-operation with federal departments and agencies and its relations with provincial authorities and police forces was productive. Our review also showed a general willingness between CSIS and the RCMP to share information with each other.

We found some instances where, in the Committee's opinion, CSIS had retained unnecessary information. One region had collected a report that did not meet the “strictly necessary” criterion under section 12 of the *CSIS Act*. CSIS has since removed the report from its database. In another instance, some of the information contained in reports did not, in our view, demonstrate reasonable grounds to suspect serious violence or a possible threat to public safety. The Committee recommended that CSIS report and retain only the information required to meet its obligations with regard to threat assessments.

Proliferation of Weapons of Mass Destruction

Canada's efforts to prevent or at least slow the proliferation of weapons of mass destruction (WMD)—chemical, biological and nuclear—to states that do not possess them are longstanding. Although Canada does not possess such weapons itself, a national infrastructure of advanced nuclear, chemical, biotechnological and electronic industries and research facilities makes the country vulnerable to illicit procurement. The goal of the Committee's review was to assess the Service's performance of its function to advise the Government in a clearly vital area.

From CSIS files it was evident that, because of consistent attempts to procure WMD, a certain foreign country was a particular focus for the Service's investigative efforts. Based on an extensive review of the documentation, we concluded that CSIS had reasonable grounds to suspect a threat to the security of Canada.

It is evident to the Committee that the Service plays an important role in Canada's management of proliferation issues at the domestic level (co-operating with police and other enforcement agencies), and globally (acting in support of DFAIT counter-proliferation initiatives, and exchanging information with allied governments and other parts of the international antiproliferation regime). We noted that, overall, the Service's approach to proliferation matters was both strategically sound and flexibly managed.

Audit of CSIS Activities in a Region of Canada

INTERNAL SECURITY

We determined that the office's internal security practices and procedures were generally sound and noted that in response to incidents elsewhere in recent years, the Region had implemented CSIS Headquarters's new procedures in relation to managing classified documents and electronic storage media.

The Committee did note, however, that the Region had conducted significantly fewer (in proportion to the staff complement) random searches of employees entering or leaving Service premises than CSIS offices in other regions. Given the security breaches of recent years, and the Service's acknowledgment of the role of random searches in increasing "security awareness" among its employees, the Committee believes the Region should bring its security practices into line with other of the Service's regional operations.

The Committee recommends that the Region increase the number of random searches to reflect the current practices in other CSIS regional offices.

Collection of Foreign Intelligence

MINISTERIAL REQUESTS

A 1987 tri-ministerial MOU stipulates that any section 16 request likely to result in the inadvertent interception of communications to which a Canadian is party, should so state. Although all Ministerial requests since August

1998 have contained such clauses, the Committee believes the declaration used currently concerning incidental interception requires additional clarification.

The Committee recommends that in requesting section 16 assistance, Ministers indicate explicitly those instances where there is a real likelihood that the communications of Canadians will be subject to incidental interception as part of the collection activity.

A related concern arises with respect to CSIS warrant applications resulting from section 16 requests. Two applications examined by the Committee did not include, as stipulated in the tri-ministerial MOU, the mandatory caution against directing the collection of information at citizens, companies and permanent residents.

The Committee strongly recommends that all future CSIS section 16 warrant applications contain the required prohibition against directing the collection of information at Canadian citizens, companies or permanent residents.

REPORTING OF SECTION 16 INFORMATION

The Committee also reviewed CSIS reports to requesting Ministries based on section 16 collection. Some contained information about Canadians that went beyond that necessary for the understanding and exploitation of the intelligence. Although these represented only a very small fraction of the total, the Committee believes that the Service could be more circumspect with little or no penalty to the quality of its analyses.

The Committee recommends that CSIS ensure that it is more circumspect and that reports to requesting agencies contain only that information absolutely essential for the exploitation of the foreign intelligence.

Appendix D

Complaint Case Histories

Complaint Case Histories

This section describes complaint cases submitted to the Review Committee during the past year on which decisions have been reached. Not addressed are complaints that were handled through administrative review, were misdirected, were outside the Committee's mandate, or on which decisions have yet to be rendered.

Where appropriate, complaints are investigated through a quasi-judicial hearing presided over by a member of the Committee. After the hearings are complete, the presiding member provides the Solicitor General and the Director of CSIS with a decision. The complainant also receives a copy of the decision, after any information with national security implications has been severed from the document.

Of the four cases described below, three involve complaints pursuant to section 41 of the *CSIS Act*, and related to the Service's role in conducting security screening investigations on behalf of Citizenship and Immigration Canada (CIC). The fourth complaint was brought under section 42 of the *Act* by a federal government employee who was denied an upgrading in security clearance level.

Case #1

The complainant has been in Canada since 1988 and was granted permission to stay in Canada on humanitarian and compassionate grounds. He had applied for permanent residence and in October 1996, the Service forwarded its advice to CIC on his admissibility to Canada as defined under s.19 of the *Immigration Act*.

The complainant is a vocal supporter of an overseas nationalist movement. Nonetheless, following fifteen days of hearings and a careful review of all of the documentary and testimonial evidence, the Committee found no concrete evidence that the complainant is or ever was a member of a recognized terrorist organization. The Committee found that the Service's reports on its interviews of the complainant contained material inaccuracies about the complainant's replies to important questions, and relied on statements supposedly made by the complainant that were inaccurately recorded.

The Committee subsequently recommended that the Service inform CIC of the Committee's findings and of the Committee's recommendation that the complainant's application be processed for landing. This recommendation was in accordance with the terms of reference agreed to by all parties in advance of the hearing.

Case #2

The second complainant came to Canada in 1991. He was recognized as a Convention refugee and applied for permanent resident status. In 1995, the Service forwarded its advice to CIC on the complainant's admissibility to Canada as a permanent resident.

The complainant was described by the Service as a member of a terrorist organization who lied about his membership when he was interviewed by the Service. The two CSIS investigators believed that they had strong

evidence to support their conclusion. The Service relied on the fact that the complainant had indicated his support of the organization, had associated with alleged members of it and was described by another person (who was himself reporting hearsay information) as a member.

The nature of the Service's interview itself became a significant issue in this case. The Service's view is that these interviews are part of an investigatory process, and provides some of the factual basis for CSIS' report to immigration. The investigator stated in his testimony to the Committee that he felt no obligation to discuss the Service's adverse information about the complainant with him because "we [were] just gathering information, . . . not making a decision." It is the Service's view that in such situations the applicant has the full responsibility for explaining the nature of his political activities and that the Service has no obligation to raise its concerns with the applicant.

The Committee does not agree. Rather, we believe that this approach does not give due consideration to the potential impact of a security screening interview, and is not in accord with the view it expressed in an earlier case, that the Service has a duty to "provide an opportunity for the prospective immigrant to explain adverse information."³² It is clear to the Committee that in this case, the complainant was never provided such an opportunity.

Although we believe the Service's initial interest in the complainant was reasonable, given the complainant's activities in support of the overseas nationalist movement, the Service's investigation failed to produce information which would constitute "reasonable grounds" to conclude the complainant was a member of the terrorist organization.

The Committee recommended that the Service inform CIC of the Committee's findings and of the Committee's recommendation that the complainant's application should be processed for landing. This recommendation was in accordance with the terms of reference agreed to by all parties in advance of the hearing.

Case # 3

The complainant arrived in Canada in 1994, was granted Convention refugee status and applied to become a permanent resident.

In 1997, the Service forwarded its advice to CIC on the complainant's admissibility. The advice sent to CIC by the Service was based on a comparison of three documents: the personal information form (PIF) completed by the complainant when he claimed Convention Refugee Status; the immigration form completed by the complainant when he applied for permanent residence status; and, the CSIS report consolidating the notes of the two CSIS investigators who interviewed the complainant.

The Committee found the Service brief to be biased and full of conjecture, often repeating the same point as if to give it more weight. The Committee's investigation revealed that some of the Service's assertions lacked substantiation and some damaging allegations about the complainant were found to be untrue. The Service had not attempted

to verify the complainant's alibi for his alleged activities which were of concern to the Service. In addition, the Service's advice was sent to CIC twenty-seven months after it interviewed the complainant and the information reported was out of date.

The Committee was also concerned by two other anomalies: CSIS investigators never provided the complainant with an opportunity to know and respond to the adverse information they held, and discrepancies identified by the analyst between the various information forms were not put to the complainant for clarification. The Committee also learned that one of the two CSIS investigators working on the case had limited knowledge of the emigré culture, the terrorist organization and of which cultural organizations in Canada were pro- or anti-terrorist organization in question.

The Committee had no reason to disbelieve the complainant's account of his experiences in another country. Furthermore, the Immigration Refugee Board, the expert tribunal in this area, ruled that the complainant had a well-founded fear of persecution. The Committee was concerned to learn that the findings of the Immigration Refugee Board had been discarded by an analyst who had never met the complainant.

In sum, the Committee saw no evidence to indicate the complainant had ever been anything other than a peaceful and law-abiding individual. After an extensive review of all available documentary evidence and of the testimony adduced during six days of hearings, the Committee recommended to the Solicitor General that the Service inform CIC of the Committee's findings and of the Committee's recommendation that the complainant's application be processed for landing. This recommendation was in accordance with the terms of reference agreed to by all parties in advance of the hearing.

These three cases shared some characteristics in common, leading the Committee to findings and recommendations that were applicable to all:

- Individuals required to attend an immigration security screening interview with CSIS investigators should receive written notice of the date and time of the interview two weeks in advance of the scheduled interview dates³³ and the notice should specify the purpose of the interview, that it will be conducted by CSIS investigators and that the applicant has a right to attend with counsel or another representative. The notice should also inform applicants that its assessment as to whether to recommend the granting or denial of an application rests on sufficient information being provided by the applicant.³⁴
- (Applicable to cases 1 and 2 only) All immigration security screening interviews be recorded and the recording retained until a decision is made by CIC on the Service's advice regarding the application.³⁵ If the Service makes a negative recommendation, the recordings should be kept until the immigration status of the applicant is determined.³⁶
- The Committee found that criteria for what constitutes "membership" in an organization were applied by the Service in such a way as to cast an overly broad net, with the result that politically active but peaceful and law-abiding nationalists were labelled as "terrorists." For security assessments under the *Immigration Act*, it is

the Committee's view that evidence of commitment or devotion to the cause and evidence that the person is prepared to respond positively to directions from the organization should be the major indicators of membership. The Committee believes the Service weakens its legitimate focus on terrorism when it extends the definition of membership in an "organization engaged in acts of terrorism" to include people like the complainants in these three cases.

- The Committee recommends that when the briefing unit of the Service's Immigration Security Screening Branch is preparing to issue a report to CIC, it draw together in committee the investigator who has interviewed the person, an investigator from the relevant operational desk, an officer not involved in the case to challenge adverse findings, and the Service's Legal Services Branch for the purpose of assessing the information, and ensuring uniformity and accuracy in the brief forwarded to CIC.³⁷
- The Committee believes that information potentially leading to proceedings against an individual must be subject to the highest level of scrutiny for credibility and reliability.

Case #4

This case differs from the first three and concerns the Service's role in providing government security assessments. The complaint was lodged by an individual pursuant to section 42 of the *CSIS Act*.

In 1996, the complainant's position within a small government agency was declared surplus and a new position was found for the complainant requiring a level II security clearance. In July 1997, the Service recommended that the complainant be denied the necessary security clearance upgrade. The Deputy Head of the agency concerned accepted the Service's recommendation and informed the complainant that he would not receive a security clearance because the complainant's activities in Canada focused directly and indirectly in support of a recognized terrorist group operating overseas.

The complainant was very active as a leader in an ethnic community in Canada. He was a high profile advocate for a peaceful solution to the conflict in a foreign country and openly lobbied politicians and diplomats to this end. The complainant was never clandestine or even secretive in his activities on behalf of the ethnic community.

The terrorist group is recognized as a particularly ferocious one, which has few scruples about undertaking any action to advance its cause. As the Service's principal objective in the security clearance process must be the protection of the nation, in marginal cases the Service may be inclined to recommend against granting a clearance, based upon the principle that the only level of risk that is acceptable is zero. In investigating this particular case, the Committee also took into consideration the fact that in other cases the Service had recommended granting security clearance to persons "associated" in one way or another with persons or groups considered a security threat, including the group at issue, because of the special circumstances involved.

With respect to the issue of association, the Committee believes that incidental association alone is not sufficient grounds to recommend a security clearance denial. There must also be evidence to support the reasonable belief

that the individual may act or may be induced to act in a way that constitutes a threat to the security of Canada. Incidental association in itself does not constitute such evidence.

Following seven days of hearings during which extensive documentary and testimonial evidence was adduced, the Committee found that the evidence presented failed to establish reasonable grounds to believe that the complainant posed such a threat. The Committee found the Service's conclusions with regard to the complainant were unwarranted — the result of misinterpreted events combined with speculation. The CSIS report to the agency concerned contained several very improbable allegations and conveyed a negative view of the complainant's reliability that was largely unsubstantiated.

While the Committee could not say what conclusion the Deputy Head would have reached had a different report been provided, the points we identified as determinative of the Deputy Head's decision were found to be poorly supported or not supported at all. It is conceivable, therefore, that the Deputy Head's decision would have been different had the Service delivered a less tendentious brief. The Committee found nothing in the complainant's political convictions or actions in pursuit of those convictions that should have caused the Deputy Head to deny the security clearance upgrade.

The Committee recommended that in future the Service prepare official transcripts of the security screening interviews it conducts or, alternatively, prepare a written summary for signature by the interviewee.

Notes

Notes

1. “Spy probe of China was aborted, Project examined Beijing’s role in Canadian business and politics,” *Globe & Mail*, September 30, 1999.
2. See “CSIS Cooperation with the RCMP—Part I,” 1997–1998 SIRC *Annual Report*, and “CSIS Cooperation with the RCMP - Part II,” 1998–1999 SIRC *Annual Report*.
3. During the course of its review, the Committee was able to reconstruct the identity of some of these (Sidewinder first draft report, for example), by gaining access to various Sidewinder files the RCMP had retained.
4. The Committee learned quite late in the course of its inquiries that unbeknownst to CSIS management, a Service employee had retained in his own files a copy of the first draft Sidewinder report and some supporting documents.
5. “Project Sidewinder Analytical Project Plan,” March 1997.
6. Measures adopted during the G7/P8 Ministerial Conference on Terrorism, Paris, June 1996.
7. Specifically, provisions in the *Canadian Charter of Rights and Freedoms* and certain limitations inherent to the *Criminal Code*.
8. See “CSIS Cooperation with the RCMP—Part I,” SIRC *Annual Report* 1997–1998, pp. 30–31.
9. CSIS exchanges information with these domestic agencies for purpose of threat assessments.
10. “Proliferation Issues,” *Background Series*, CSIS, no. 7, May 1999.
11. “Sensitive institutions” refers to trade unions, the media, religious institutions and university campuses.
12. A replacement warrant is required when the Service changes the targets, the places or the powers of an existing warrant, or when an existing warrant expires and the Service wishes to continue the investigation using methods for which the Court’s approval is necessary.
13. EXIPC was created in 1987 and had rarely met in recent years.
14. Following a formal request by the RCMP, CSIS discloses information or intelligence in a format that protects the identity of sources and the methods of operation. The disclosure includes a provision directing that the information be used only for investigative leads, not in judicial proceedings.

15. Following a formal request by the RCMP, usually subsequent to a disclosure letter, CSIS Headquarters gives permission to use Service information in judicial proceedings such as warrant applications and evidence at trial.
16. “*National Security Offenses Review Report*,” RCMP Audit and Evaluation Branch, June 17, 1999.
17. *CSIS Cooperation with the RCMP - Part I*, October 16, 1998; *CSIS Cooperation with the RCMP—Part II*, February 12, 1999 (SIRC Study 1998-04); and *Review of Transnational Crime*, (SIRC Study 1998-01) August 25, 1999.
18. A dormant arrangement is one in which there has been no contact for one year or more. Liaison arrangements become dormant for a number of reasons: a simple lack of need to exchange information, concerns by the Service about the other agency’s professional or human rights practices, or an assessment that the political situation in the other country is too unstable.
19. The Communications Security Establishment is an agency of the Department of National Defence. As described by the Communications Security Establishment Commissioner in his 1999–2000 *Annual Report*, the CSE “provides the Government of Canada with foreign signals intelligence (SIGINT) which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions . . . the CSE also provides advice on the security of the government’s information technology.”
20. The format and content of Ministerial requests for assistance is governed by the 1987 tri-ministerial agreement on section 16 activities. “Memorandum of Understanding on Section 16 of the *CSIS Act*,” signed by the Minister of Foreign Affairs, Minister of National Defence and the Solicitor General.
21. This number includes 6701 requests for security screening of applicants based in the United States.
22. When the Service believes that it is not in a position to render a recommendation to CIC concerning a citizenship application, it must seek approval from the Solicitor General to continue investigating the case and “defer” providing the assessment.
23. This number includes the 4415 requests for assistance.
24. The majority (81) of applicants were from within Canada, whereas only 28 were overseas applicants.
25. The Bench was composed of Justices Linden, Robertson and Sharlow. Justice Sharlow rendered the reasons for judgment of the Court.
26. R.S.C. 1985, c.1-2.

27. Gibson J. refers to the following quote, found at [1996] 1 F.C. 174 (F.C.T.D.) at 241, as the grounds for the decision of MacKay J.: “. . . paragraph 19(1)(g), in so far as it relates to “persons who there are reasonable grounds to believe . . . are members of . . . an organization that is likely to engage in . . . acts” (“of violence that would or might endanger the lives or safety of persons in Canada”), contravenes paragraph 2(d) of the *Charter of Rights and Freedoms* [hereinafter the *Charter*] which ensures, to every one, freedom of association. I find it is not established that this limit freedom under the impugned portion of the paragraph in issue is a reasonable limit demonstrably justified in a free and democratic society. I note that this determination does not relate to other classes of persons described in paragraph 19(1)(g) of this Act.”
28. More specifically, it was argued that the use of “subversion” and “democratic government, institution and processes” in section 19(1)(e) is “vague and not capable of being given a consistent and settled meaning” and is therefore inconsistent with section 7 of the Charter and the principles of fundamental justice; that the term “subversion,” as used in section 19(1)(e), infringed Mr. Yamani’s freedom and equality rights under sections 2 and 15 of the *Charter* by being overly broad and lacking “definitional boundaries” and that the phrase “reasonable grounds to believe” in sections 19(1)(e) and (g) established an “illusory standard of defense” which violated the principles of fundamental justice under section 7 of the *Charter*.
29. Gibson J. held the phrase “subversion” was “incapable of framing the legal debate in any meaningful manner or structuring discretion in any way” and thus infringed on Mr. Yamani’s rights under section 7 of the Charter, however, it was saved under section 1 of the Charter as reasonable, prescribed by law and demonstrably justified in a free and democratic society. The court also found “subversion” was not so lacking in definitional boundaries and overly broad to result in an infringement of freedom and equality rights under sections 2 and 15 of the Charter. Regarding the phrase “democratic government, institutions and processes,” the court held it was not so vague as to be incapable of being given a consistent and settled meaning, nor is it lacking in definitional boundaries or overly broad. He found no merit in the argument that the phrase “reasonable grounds to believe” provides an “illusory standard of defense” and held its use was not inconsistent with the principles of fundamental justice under section 7 of the Charter.
30. *Shandi (Re)* (1992), 51 F.T.R. 252.
31. Gibson J. noted that Mr. Yamani’s testimony indicated “evasiveness and a willingness to lie” and quoted the following from Mr. Yamani’s testimony (which he found at p.17 of the Committee’s Report): “As a Palestinian who lives in Lebanon and was born in Lebanon, I am not allowed to go back to the West Bank, and I am not allowed, maybe in two years, to go back to Lebanon. I might be deported from Canada. You do not want me to lie? To survive as a human being and to survive for my children, no, I will lie and I will lie and I will lie to protect myself. And I will lie without hurting anyone because I told you, I am not that kind of person who is stupid to go and do whatever activities.”

32. SIRC *Annual Report*, 1997-1998, p. 11.
33. The Committee has been informed that CSIS and CIC have implemented this recommendation and now provide two to eight weeks written notice, depending on the location, and that the convocation letter specifies that the interview will be with a CSIS employee. It is Service policy not to raise objections to the presence of a third party observer.
34. The Committee recommends that the notice refer to the legislative mandate and state that the Service will be conducting the interview in order to issue advice to CIC in determining the applicant's admissibility in light of the inadmissibility classes of section 19 (1) of the *Immigration Act* and the definition of "threat to the security of Canada" as defined in the *CSIS Act*.
35. This recommendation was also made in the report *In Flux But Not In Crisis* by the House of Commons Special Committee on the Review of the *CSIS Act* and the *Security Offences Act*, September 1990.
36. The Service's policy states: "An interview with an immigration applicant may be taped by an investigator only with the consent of the applicant or under the authority of a warrant. The investigator must not object should an applicant wish to tape an interview. In such circumstances, the investigator should also ensure the interview is taped". The Service contended that, as consent would not be forthcoming in all cases, this recommendation could not be equitably applied.
37. The Service's process has been changed since the issuance of the Committee's reports. Currently, reference material used to provide information and advice to CIC is scrutinized for accuracy under a three-tier review mechanism. This mechanism also provides for regular consultation with the Counter Intelligence Branch (CI) and Counter Terrorism Branch (CT) subject matter experts and, as required, by legal counsel. The Service believes it has sufficient levels of control in place to ensure accuracy, thoroughness and efficiency.