Section 1: A Review of CSIS Intelligence Activities

A. Areas of Special Interest for 1998-99

As has been the practice in recent Annual Reports, the results of special inquiries and concentrated research carried out by the Committee in the course of the year begin our report. These special studies are an addition to and are intended to reinforce the other forms of audit research the Committee undertakes.

Review of Transnational Criminal Activity

Report #107

Organized criminal groups have long been a concern of many democratic governments because of their capacity to disrupt and destabilize the economic well-being of the countries in which they operate, and the threat they pose to law and order. In recent years, criminal organizations both old and new have taken advantage of the greatly increased mobility of populations and advances in communications technology, to extend their activities internationally. In the decade since the end of the Cold War, the activities of the criminal groups emerging from the nations of the old Soviet empire have been of particular concern.

The seriousness of this growing phenomenon was recognized in 1995 when the G-7 states formally recognized international organized criminal activity as a threat to their security. Many more nations have since strengthened their enforcement efforts, and when they can, have turned to available national security and intelligence resources to assist police in combating the threat.

The Origin of the Service's Interest in Transnational Crime

Following a 1993 Department of Justice legal opinion which embraced the view that transnational criminal activity in certain of its forms could represent a threat to the security of Canada, a role was identified within the Service's mandate whereby CSIS could assist domestic police authorities.[2] This new CSIS role represented a significant departure from the Service's traditional area of responsibility in which criminal activities were generally investigated only in the context of espionage and serious politically-motivated violence.

Commencing in 1995, the Service initiated a number of investigations into transnational criminal activity using targeting authorities which named individuals, and generic approvals where individuals were not named.[3] From the outset, the Service's role was limited to the collection of strategic intelligence. Involvement in criminal matters of a tactical nature more properly the responsibility of police or other law enforcement agencies was to be avoided. The Service's Regions were provided with a set of key objectives for the investigation of the issue-based target (to be discussed more fully below)—objectives which reflected the strategic thrust of the Service's program.

The Service also identified six conditions under which the activities of transnational

The activities of the criminal groups emerging from the nations of the old Soviet empire have been of particular concern.

criminal groups could be said to represent a threat to the security of Canada. International crime was a threat to Canada when it impacted upon,

- law and order to the extent of affecting the fabric of Canadian society;
- Canada's economic security through such things as large-scale money laundering;
- government programs such as immigration and refugee processes;
- the government's negotiating position with foreign countries;
- Canada's foreign policy interests; and,
- government institutions through such activities as the corruption of public officials.

It was evident to the Committee that CSIS investigators lacked the training and experience to recognize the types of financial and corporate crimes that were supposed to be the object of concern.

The first task CSIS set for itself was to establish a solid data base on all the various manifestations of transnational crime. Investigators were authorized to interview persons who may have held relevant information. The Service also made use of its extensive liaison arrangements, both domestic and foreign, to solicit information on the phenomenon generally, and on individuals suspected of being involved.

The focus on the collection of strategic intelligence was restated by CSIS management in November 1997 with investigators urged to make every effort to avoid areas of investigation which fell below the Service's threshold or which had an imminent probability of developing into an enforcement investigation. The Service also took pains to explain its role to domestic government and police agencies, and also to collaborating security/intelligence agencies overseas. In the latter case, CSIS Security Liaison Officers were instructed to make it known to their foreign counterparts that despite its own strategic focus, the agency was able to "broker" tactical information on transnational criminal activity between them and Canadian enforcement agencies.

Methodology of the Audit

The Committee's 1997-98 audit report examining the Service's cooperative relationship with the RCMP noted CSIS' new initiatives in the area of transnational crime and we stated our intention to conduct a specific inquiry into the Service's activities. The review, the results of which are presented below, was carried out in order to ensure that CSIS investigative activities in relation to transnational crime were consistent with its mandate under the law, its operational policies, and Ministerial Direction.

In selecting cases for special study, our aim was to encompass the spectrum of Service activities: thus we chose an issue-based investigation, an investigation of a foreign-based criminal group in Canada, and the investigation of an individual with suspected links to a foreign criminal group. SIRC researchers examined all files, reports, memoranda, and other documents relating to the selected cases, as well as all policy decisions and instructions governing transnational criminal activity generally.

Findings of the Committee

Training Relevant to the Specialized Nature of the Crimes Involved

The Committee identified several problems that arose quite early in the Service's program. First, it was evident to the Committee that

CSIS investigators lacked the training and experience to recognize the types of financial and corporate crimes that were supposed to be the object of concern. Sophisticated criminal activities such as money laundering, manipulation of international capital flows, securities fraud, and high-level corruption were new to investigators. The Committee's inquiries showed that some thirty months into the program, Service officers were still complaining about their lack of training and some stated that they did not know how to identify certain forms of criminal activity.

"Strategic" and "Tactical" Investigations—a Threshold That Works?

A second problem stems at least in part from the first: the Committee saw that a number of CSIS investigations and inquiries resulted in the collection, retention, and reporting of information on tactical, street-level criminal activities that were clearly not within the scope of the Service's strategic objectives. We believe this results from the fact that the investigative threshold meant to distinguish strategic from tactical intelligence was never adequately defined.

In our review of CSIS cooperation with the RCMP (contained in the 1997-1998 Annual Report) we stated our belief that the terms *strategic* and *tactical* when used in relation to the investigation of transnational criminal activity, were not defined such that they would serve to identify a particular role for the Service. The potential for this sort of overlap was recognized by the Service itself in late 1997. One CSIS official noted that the Service found it difficult to avoid the collection of tactical information which would normally be the province of the police of jurisdiction. It continues to be the Committee's view, therefore, that where CSIS is unable to bring a unique perspective to a specific area involving transnational crime, it should leave the matter in the hands of the appropriate law enforcement agencies.

Nature of Cooperation Between CSIS and Overseas Agencies

The Committee's third general concern touches on the Service's international contacts. Its focus on strategic intelligence had an unanticipated impact on relationships with collaborating foreign security and intelligence agencies. CSIS learned over time that these agencies were interested in tactical intelligence on transnational crime in support of law enforcement organizations in their own countries. In spite of the Service's offer to serve as a link to the Canadian agencies concerned, the overseas security and intelligence agencies—working partners with CSIS of long standing—established their own direct links with Canadian law enforcement agencies. The intelligence "brokering" role that CSIS saw for itself did not develop as planned and the Service was to some extent left out of the intelligence information exchange.

CSIS Contribution to Canada's Fight Against International Crime

The Committee's review identified several instances where the collection by the Service of strategic information (and its subsequent dissemination to the appropriate government agencies) played a crucial role in government decision making. In addition, the Service's strategic data base on transnational crime aided Citizenship and Immigration Canada

Where CSIS is unable to bring a unique perspective, it should leave the matter in the hands of the appropriate law enforcement agencies.

in preventing the entry into Canada of certain organized crime figures based overseas.

The question arose in an earlier review (See 1997-1998 SIRC Annual Report, page 32) as to whether CSIS was providing the RCMP with all the information it had on transnational criminal activity. During the period reported on here, the Committee found that for the most part all tactical or other criminal information that was collected in the course of its strategic investigations was passed promptly to the RCMP or to the police force having jurisdiction. While SIRC researchers did come across a number of tactically relevant reports that bore no positive indication of being passed to police authorities, it was not possible to determine whether the contents of the reports had been provided to police verbally.

The Committee was encouraged to note the increasing flow of information from CSIS to departments and agencies of government having particular responsibilities for foreign trade and economic development.

Domestic Liaison Matters Requiring New Policy Direction or Clarification

The existing liaison arrangements between the RCMP and CSIS provide for an exchange of liaison officers at the national and regional headquarters level. By virtue of the RCMP's responsibilities under the *Security Offences Act*, RCMP liaison officers are provided access to all reports that relate to the Service's Counter Terrorism Program originating from the headquarters to which they are attached. However, the Service's transnational crime investigations are conducted not by its Counter Terrorism staff, but rather by its Counter Intelligence officers—whose product is not routinely available to the RCMP in all regions. It is thus left to Service personnel in some regions to assess the incoming transnational crime intelligence and determine its relevance to the RCMP.

It is the Committee's view that the current administrative division of labour holds out the possibility of inadvertent failure to pass on important information to the RCMP. We believe that Service policies should be reviewed to eliminate that possibility.

The Committee was encouraged to note the increasing flow of information from CSIS to departments and agencies of government having particular responsibilities for foreign trade and economic development. The advice provided to these agencies assists them in ensuring that foreign criminal groups do not become involved in, or derive benefit from, Government of Canada programs.

One instance that did raise a note of caution concerned a serious case where a fraud involving several million dollars may have prompted a government agency to seek the Service's help. In the request for assistance there was the implied expectation that in the future, in order to ensure that there were no transnational criminal connections involved in joint ventures with foreign parties, the Service would routinely conduct background checks on companies and individuals seeking the government agency's financial backing.

While there seems to be no reason why adverse information already in the Service's possession should not be provided to the agency, in our opinion there is no legal basis for the Service to initiate such inquiries without there being reasonable grounds to suspect that there is a threat to the security of Canada. It is the Committee's view that a clarification in written policy would help ensure that no inappropriate investigations are undertaken in similar situations.

The "Issue-based" Investigation

The use of generic, or issue-based targeting authorities by the Service, enables it to investigate a class of threat activity, or a particular group or organization, where there are reasonable grounds to suspect that the activities represent a threat to the security of Canada, but where the identities of the individuals involved may not be known.

The generic targeting authority in the case we examined was intended to give CSIS the means to obtain a strategic overview of transnational criminal activities linked to a specific group of countries. It is the Committee's view that as a general rule, once the identity of an individual becomes known through the use of a generic targeting authority (and there exist reasonable grounds to suspect that the person's activities represent a threat to the security of Canada) the Service is obligated to obtain a specific targeting authority in order to continue an investigation of that individual. Our review of the general targeting authority came across two instances where investigative activity was continued against known individuals under the generic targeting authority.

In the first case, after establishing the identity of an individual under the generic targeting authority, the Service continued to investigate and collect information on that person. Our review of the documents indicates that there probably were sufficient grounds to suspect the individual of threat activities, in which case a new, specific targeting authorization would have been justified. The Committee believes that the Service's continued investigation of the individual in the absence of such authorization may have been an inappropriate use of issue-based targeting.

In the second case, instructions from CSIS Headquarters were sent to a number of regional offices to collect certain information under the generic targeting authority. One office questioned whether the generic authority was sufficient to collect the requested information and was informed that a specific targeting authority would indeed be sought.

This instance raised two issues for the Committee. The fact that the specific authority was obtained only after the original headquarters request was questioned by a regional office indicates that there may be gaps in the articulation and comprehension of the Service's policy concerning issue-based targeting and transnational criminal activity. We were informed that the CSIS *Operational Policy Manual* includes no such specific policy instructions. The Committee believes these omissions should be rectified. Secondly, the nature of the response by headquarters to the regional office query revealed a perspective on the use of issue-based targeting which was not supportable, in the view of the Committee.

There may be gaps in the articulation and comprehension of the Service's policy concerning issue-based targeting and transnational criminal activity.

The Specific Investigations

The two specific target authorizations the Committee reviewed were a known foreign criminal organization and an individual with suspected links to it. The activities attributed to the individual included an alleged major fraud against an agency of the Canadian government. Given the extent and complexity of the activities involved,

the Committee believes that a foreign influence case against the individual had yet to be made. Should no clear foreign influence be established, and the suspected criminal activities be on his own behalf, it is our view that any further investigation should be a matter for the police.

The question of whether CSIS' mandate permits its involvement in the investigation of transnational criminal activity remains open at the present time.

Other Countries' Handling of Transnational Criminal Activity

Documents collected by CSIS and read by the Committee during the course of its review provided insight into the way several allied security and intelligence agencies investigated transnational criminal activity. To a large extent, the investigative activities of these foreign agencies were "client-driven"—the client being either the police or a national criminal intelligence organization. With one exception, intelligence agencies concentrated on gathering information intended to be used in direct support of law enforcement measures. CSIS pointed out that it assisted law enforcement as well as other Federal departments and agencies in a similar fashion.

Conclusions and Recommendations

From the Committee's perspective, the question of whether CSIS' mandate permits its involvement in the investigation of transnational criminal activity remains open at the present time. In the coming months, we will present our views on the issue.

The Committee believes that the problems CSIS has encountered in this area can be attributed, at least in part, to the lack of familiarity and experience which naturally accompanies venturing into a new field. In the event that the Service continues to be involved in this sector, we believe several measures are warranted.

The threshold for CSIS intervention ought to be clearly articulated: Service participation should be contingent on the criminal activity being of such seriousness and scope as to represent a genuine threat to the strategic, social, economic, and national security interests of Canada. The Service should not become involved in the investigation of criminal activities best left to law enforcement agencies.

There is a larger public policy question to be addressed by Government. Currently, CSIS is following Ministerial instructions to deal with issues of international crime. However, our reviews indicate that the Service may not be equipped either by tradition or by training to take on the task. Given the importance of the matter, we would urge the Government to consolidate and clarify its intentions on how to address this growing array of threats to Canada.

Should CSIS continue to remain involved in the area, the Committee recommends that,

> it develop a clear operational policy in all its aspects for investigating transnational criminal activity. Such policy should include the requirement to assess each case whenever consideration is given to initiating an investigation under an issue-based targeting authority; and,
>
> it implement a program of special-

ized training in the key areas of transnational crime in order that the objective of providing strategic intelligence to the government on major international criminal activities can be fully realized.

Review of Intelligence Production

Report #110

The Service's primary mandate has two key elements: first, to "collect, analyze and retain information and intelligence" on threats to Canada, and second, to "report to and advise the Government of Canada" on these matters. Within CSIS, Counter Intelligence and Counter Terrorism branches perform the collecting function, while Requirements, Analysis and Production (RAP) Branch has a major, though not exclusive, role in producing reports and advice. The RAP Branch is thus one of the transmitters of information between the gatherers of data and intelligence and the rest of the Service, and between CSIS and the rest of Government. As part of the 1998-99 research program, the Committee undertook to review the activities of the RAP Branch of CSIS.

Methodology of the Audit

Between September and November 1998, SIRC researchers interviewed RAP personnel at all levels to learn about the Branch's structure, its production processes, and the manner in which priorities are set and implemented. We reviewed the advice that the Service provided to Government by examining selected statements from *CSIS Reports* and *Intelligence Briefs* prepared by RAP during fiscal year 1997-98, and comparing them with the source material used in their creation. We also interviewed a wide range of RAP's clients outside the Service to determine whether their intelligence requirements were being met.

Previous Studies

Serving as a valuable baseline for this year's review of RAP were two previous studies.[4] The first was carried out by the Independent Advisory Team (IAT) in 1987 headed by the Honourable Gordon Osbaldeston. The IAT observed in what was then called the Intelligence Assessments Branch (IAB) serious organizational deficiencies that affected the quality of intelligence production. At that time, CSIS research and analysis functions (operational analysis, strategic analysis, and "research") were carried out in three separate directorates. Coordination was difficult and had a negative impact on the Service's ability to produce intelligence that adequately responded to Government needs. Osbaldeston's team recommended an amalgamation of all three components into one functional unit.[5]

The IAT report also highlighted the absence of clearly defined intelligence priorities, the lack of a coordinated system for production, and inadequate reference facilities. Too much emphasis, it said, was placed on the short-term analysis of events as they unfolded, and too little on longer-term analysis that would help the government develop policy and make strategic decisions. Osbaldeston recommended that CSIS develop a strategic plan for intelligence production based on the Government's intelligence priorities, and adopt an inte-

The RAP Branch is thus one of the transmitters of information between the gatherers of data and intelligence and the rest of the Service, and between CSIS and the rest of Government.

grated approach to the collection, analysis, and dissemination tasks.[6]

The second study was conducted by the Committee one year later. Our in-depth review in 1988 found that the operational branches remained preeminent in the intelligence production process, one result of which was the continued over-emphasis on short-term intelligence to the detriment of strategic analysis. Two key recommendations emerged from the review. We recommended that CSIS management decide whether to continue with the status quo or take the active steps necessary to develop a strategic analysis capacity.[7] In addition, we suggested that the Intelligence Assessments Branch undertake to recruit outside professionals with experience in strategic intelligence and knowledge of the social and cultural backgrounds of CSIS targets.[8]

CSIS needs to take greater care in distinguishing between "analysis" and statements of fact in its products.

RAP Today

In 1992, the Service addressed most of the points raised by the IAT and our own audit in a reorganization of the Intelligence Assessments Branch. Renamed the Requirements, Analysis and Production Branch, RAP created first a Strategic and Emerging Issues Section to conduct strategic analysis and focus on emerging security intelligence issues, and later a Marketing and Client Relations Unit to respond more effectively to the Government's requirements.

Since the critical restructuring of 1992, there have been additional changes to the way RAP functions. Previously organized along geographic lines, RAP's structure mirrors more closely that of the other operational branches in order to eliminate duplication of research and more clearly develop expertise. The Strategic Analysis Unit that provided longer-range analysis to the Government was recently disbanded to allow the integration of strategic analysts into operational areas.

Findings of the Committee

Client Assessment of RAP Products

We examined the quality of reports produced by RAP. Selecting statements from ten branch products not self-evidently supported by the rest of the text, we then examined the documents employed as source material. The overall conclusion we were led to was for both internal and external clients, CSIS needs to take greater care in distinguishing between "analysis" and statements of fact in its products.

We interviewed a number of RAP clients in order to gain insight into consumers' views of Service intelligence products. Generally the comments were positive: "CSIS Reports are clear, well written, easy to follow, and provide good background information on a series of subjects." Service reporting to clients was seen to be timely, with specific mention being made of recent CSIS reports on Information Warfare. There was some concern expressed about not knowing when Service intelligence products could be expected to arrive.

On a more critical note, several clients told us that they were often in receipt of RAP products that did not directly address their departments' operational requirements. Others believed that RAP reports were

sometimes over-classified considering the information they contained, thus limiting their distribution.

Setting Branch Priorities

RAP has been in an almost continuous cycle of change during the last decade in an effort to accommodate the needs of its various clients. Despite these efforts, the influence of the operational branches predominates simply because they are the primary sources of information about threats to national security.

A number of factors led us to this conclusion. The Branch produces an annual plan that is based, in large measure, on the National Requirements that are shared by the operational branches, with the needs of external clients appearing to play little role. In addition, Government clients lack the information from CSIS that would permit informed choices about the intelligence products available. And finally, external clients when meeting with the Service to discuss their needs are told that RAP may or may not act upon a particular request. It is evident that some clients may not fully appreciate the limitations of CSIS mandate and the impact this may have on the Service's ability to act on certain requests.

While the Committee acknowledges the organizational reality that clients in Counter Intelligence and Counter Terrorism will continue to influence much of what RAP does, we remain convinced that the Service should continue its active efforts to accommodate its external partners, and that it is possible to seek a better balance without penalty to internal operations.

There is a similar lack of balance in the area of strategic analysis. Our discussions with both RAP's internal and external clients evinced the clear need for more and better long-range, strategic analysis.

In order to redress these shortcomings, set balanced production priorities, and avoid a situation where the Government is not as well informed as it should be, renewed direction from CSIS senior management is required. To this end, the Committee has two recommendations:

> the reinvigoration of an apparatus that has become defunct in recent years—the Executive Intelligence Production Committee (EXIPC).[9]

> the articulation by CSIS of a specific plan to meet the clear requirement of both internal and external clients for more strategic analysis.

Quality Control and Staff Morale

The Committee's review showed that analysts are given little formal training when they join RAP, although the Service has stated it intends to introduce formal training sessions in the near future. There are no written guidelines about how intelligence reports are to be produced, however, earlier Branch products serve as examples and senior analysts act as mentors.

Our review also identified a troubling form of professional segregation within the Branch. RAP staff who are not classified

Some clients may not fully appreciate the limitations of CSIS mandate and the impact this may have on the Service's ability to act on certain requests.

as intelligence officers (IOs) are treated differently in the areas of salary, training, and career advancement. Officers in the non-IO categories do not benefit from operational experience or foreign postings, and they are paid significantly less. We learned of the case of one non-IO staff member who after serving in an acting capacity as a manager for two years was then denied the opportunity to compete for the position. The person has since filed a grievance.

The Service should continue active efforts to accommodate its external partners, ... it is possible to seek a better balance without penalty to internal operations.

In order to address these issues, the Committee recommends,

> that the Service develop quality control guidelines and protocols for its written product, and devise methodologies for checking the veracity of information on which reports are based.
>
> that CSIS implement a comprehensive career plan encompassing all RAP officers, IOs and non-IOs alike. Ideally, the new career plan would include more scope for professional growth within the Branch while maintaining opportunities for movement within the Service, and into the larger public service when appropriate.
>
> that a reasonable proportion of supervisory positions within the RAP establishment be designated for officers in the non-IO category.

Review of Foreign Intelligence Activities in Canada

Report #115

For this study the Committee reviewed CSIS investigations of the activities in Canada of a foreign state's intelligence services. We last looked at the Service's investigations in this area a number of years ago, and now as then, the Service's investigations centered on the activities of several members of the country's diplomatic service, posted to missions in Canada and acting as declared and undeclared intelligence officers.[10]

Our audit set out to assess the threat (as described in sections 2(a) and 2(b) of the *CSIS Act*) posed by the foreign intelligence services under investigation, to determine whether the Service's investigations were proportionate to the threat, and to verify Service compliance with the provisions of the *CSIS Act*, Ministerial Direction, and CSIS operational policies.

Methodology of the Audit

The Committee's review included the following:

- a warrant affidavit and the supporting documentation, in order to ascertain the basis for the CSIS investigations;
- the Request for Targeting Authorization (RTA) which began the investigative process;
- several investigations, chosen at random, of foreign intelligence officers in Canada;
- several human source files associated

with the investigations; and,
- many of the most sensitive files held by Service in order to understand the extent of the operations conducted by the foreign state's intelligence services on Canadian territory.

The Threat

The Committee was satisfied that the documentation did support the conclusion that the intelligence services of the foreign state concerned remained a significant threat to Canada. We examined the resources directed against the threat, and certain measures of the threat itself. While assessments of the threat written by allied governments and made available to the Service contained some contradictory information, the Committee regards the level of resources devoted by the Service to the threat as appropriate.

Based on our review, the Committee agrees that the "reasonable grounds to suspect" that the foreign intelligence officers in Canada were involved in the covert collection of classified or proprietary information were present. However, in certain of the circumstances we reviewed, the threat did not appear to be particularly pressing or significant. Nevertheless, we also saw compelling and irrefutable evidence that this foreign government continued to direct significant clandestine intelligence activities against Canada.

We noted CSIS' assertion that the intelligence services under investigation were increasingly employing non-traditional techniques so as to minimize the risk of diplomatic "spy scandals" should their operations be uncovered. While the Committee believes that the use of non-traditional forms of "cover" represent a potential threat, our review of the base documentation led us to believe that this form of threat had not been established to the extent suggested by the Service.

Findings of the Committee

While we were able to draw conclusions about the overall, long-term threat to Canadian security posed by the foreign state's intelligence services, the level of threat in individual cases was less apparent. Intelligence operations are inherently protracted affairs; when coupled with the limited time frame (one year) covered by our review, definitive conclusions about the threats posed by individual targets are difficult to draw. We were, however, able to fully evaluate the conduct of the Service's investigations in relation to compliance with operational policy, procedures, Ministerial Direction, and the *CSIS Act*.

We saw compelling and irrefutable evidence that this foreign government continued to direct significant clandestine intelligence activities against Canada.

Retention of Information

The Committee identified one item of information in the Service's data base that did not meet the "strictly necessary" test for collection and retention. The information, in our view, was incidental to the investigation and unrelated to the activities of the targeted foreign intelligence services. We have so informed the Service.

Fact in a Request for Approval

In the course of reviewing base documents for a Service operation that extended over a number of years, we found an error of fact in a request for approval sent to the Solicitor

General. The request was to approve an operation and incorrectly identified the country where similar types of the operation had been successful. The correct information had been available to CSIS staff at the time of the request. We brought this to the attention of CSIS and it agreed with our assessment.

Policy in the Case of a Sensitive Operation

The Committee examined an operation against an intelligence officer posted to Canada. The officer had sought information about Government policy. As a result of our examination of the case, we concluded that a Government department should have been given certain information about the matter. Service files showed that this had not occurred. We advised the Service of our findings.

It is not unusual for persons (including Canadians and Canadian residents) in contact with known or suspected intelligence officers to be approached by the Service for information.

CSIS Contacts with Canadians During Counter Intelligence Operations

The CSIS investigations we examined were all directed at foreign nationals, however, it is not unusual for persons (including Canadians and Canadian residents) in contact with known or suspected intelligence officers to be approached by the Service for information. In one case we came across during our review, we noted the considerable efforts by the Service to explain to an individual contacted for such purpose that he was not the subject of investigation.

CSIS Investigations on University Campuses

Report #114

Security intelligence policy in Canada treats university campuses as "sensitive institutions." Investigations associated with any university, technical institute, community college or CEGEP are thus subject to policies and procedures more stringent than most other areas of Service investigation. The purpose of this study was to examine the use and effectiveness during the audit period of these additional procedures—specifically, the Ministerial Direction authorized in 1997—and to review CSIS investigative activities at post-secondary institutions for compliance with Ministerial Direction, the CSIS *Operational Policy Manual (OPS)*, the *CSIS Act*, and other relevant legislation.

Methodology of the Audit

The review covered the period 1 March 1997 to 30 September 1998 and involved examination of a broad range of Service files and documentation (both electronic and hard copy):

- Aide-mémoire on campus operations approved by the Minister; and the authorizations by the Minister, the Director of CSIS, and senior managers.
- Human Source Branch correspondence concerning policy on investigations at post-secondary institutions.
- Authorizations for investigations approved by senior CSIS managers pertaining to post-secondary institutions.
- Human Source Branch administrative

files, and source handler reports.
- section 12 data base reports about any targets of CSIS investigations who were staff, students, or employees at the post-secondary institutions.

History of Campus Investigations Policy and Practice

1963 Agreement with CAUT

Existing campus investigation policy has its origin in a 1963 agreement between the Federal Government and the Canadian Association of University Teachers (CAUT). Known as the Pearson-Laskin Accord, the agreement was a policy response to concerns about RCMP Security Service campus investigations during the 1950s and 1960s. The agreement articulated policy affirming that the Security Service would enter onto post-secondary institutions only to conduct security screening or "where there [were] definite indications that individuals may be involved in espionage or subversive activities."

The Accord noted specifically that,

> no informers or listening devices will be used on university campuses except where the Solicitor General has cause to believe that something specific is happening beyond the free flow of ideas on university campuses.

The basic message of the Accord appears to be that the Government would not engage in general surveillance of universities and colleges. The Accord contained the specific statement, "there is at present no general RCMP surveillance of university campuses."

Subsequent policies dealing with campus investigations have carried forward the principles of the 1963 agreement. They were restated in 1971 in the form of a Cabinet record, and again in 1984 when just prior to the passage of the *CSIS Act*, the Solicitor General published the Ministerial Direction, "Security Investigations on University Campuses."

Following closely the wording of the 1963 Accord, the Ministerial Direction states that security investigations on campus were only to take place where there were "definite indications that individuals may be involved in activities prejudicial to the security of Canada." The essence of the Direction was that the Minister had to approve the use of human sources and other intrusive methods on campus.

Security investigations on campus were only to take place where there were "definite indications that individuals may be involved in activities prejudicial to the security of Canada."

Application of the 1984 Ministerial Direction

By the mid-1990s it was apparent that in its application, the 1984 Ministerial Direction was flawed. Because it predated the *CSIS Act*, it employed tests, procedures, and legal terminology not found in the *CSIS Act* — the founding legislation for the new Service that had to use it.

There were also operational problems created by the need for the Service to seek Ministerial approval to investigate any and all campus activities no matter how far removed they were from the "free flow of ideas" in the academic milieu. This gave rise to an authorizing procedure not in

Lawful Advocacy, Protest, Dissent, and Sensitive Institutions

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

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

keeping with the principles of the 1963 accord. The Service disagreed and noted that successive Solicitors General have provided CSIS with the authority in question.

Both the Review Committee (in 1991) and the Inspector General (in 1995) found the policy wanting, and so stated.

Policy Revision of 1997

In 1997, the Solicitor General issued new Ministerial Direction—"Security Investigations at Post-Secondary Educational Institutions"—meant to address the problems and bring policy in line with existing legislation. The general principles of the 1963 agreement were retained, and investigations had to be consistent with the tests of the *CSIS Act*, particularly in its protection of lawful advocacy, protest, and dissent.

The 1997 Direction made two fundamental changes. The Director of CSIS was delegated the authority to approve source activities which while located on campus were entirely removed from the academic milieu. The Director was to provide the Minister annually with a "summary" of all such cases approved.

In addition, the Director was also delegated the authority to employ sources on campus in situations where there was no possibility of obtaining the prior approval of the Solicitor General. The Director was obligated to notify the Minister as soon as possible thereafter about the circumstances of the operation.

Like its predecessor, the new Ministerial Direction recognized the need for CSIS officers to visit campuses to conduct security screening investigations, but cautioned that these were not to be used as a pretext for other investigations.

Findings of the Committee

Consistency in Articulation of Policy

As a general rule, CSIS officers rely on relevant sections of the CSIS *Operational Policy Manual* which are derived from Ministerial Direction. Therefore, an examination of the Service's interpretation of

Ministerial Directions, as expressed in its policy manual, was an important part of our review. The Committee identified some potential problems:

- in instances where the Minister's approval is still needed, the policy manual excluded the requirement set out in Ministerial Direction that the Service provide an explanation to the Minister of how the proposed operation would affect the rights and freedoms of the subjects of the investigation and others associated with the institution;
- a term for a particular type of investigative activity has been subject to too broad and varied an interpretation;
- the policy contained no references to the seminal 1963 Pearson-Laskin Accord; and,
- the policy permits CSIS officers, without Ministerial approval, to go on campus to collect information for security screening purposes and for other mandated enquiries; the purpose and scope of such enquiries not being adequately defined.

Campus Investigations and Operations

During the eighteen-month period covered by the audit, there were two cases where CSIS employed its newly delegated authority. In the first, the Director of CSIS approved a procedure for the continuation of an activity that had been agreed to by the Minister the year before. The Director's decision was based on staff advice that the investigative activity would not affect the free flow of ideas and normal academic life at the institution and was thus permitted under Ministerial Direction.

The Committee questioned whether the one-year approval for the procedure was in keeping with the essence of the 1963 Accord. CSIS asserted that the authority was consistent with post-1963 legislation, Ministerial Direction, and Service policies.

We noted too that Ministerial Direction dictates that the Director report by way of summary to the Minister following operations where approval had been delegated to the Director. Apart from a one-line reference in the Director's Annual Report, the Committee could locate no other document that would indicate that the Minister had been informed of the matter—in the Committee's view, less than adequate compliance with Ministerial Direction.

The Service should be required to explain how a particular investigation will impact on the rights and freedoms of persons who are subjects of the investigation as well as those persons associated with the institution concerned.

In the second case where the 1997 Ministerial Direction had delegated authority to the Director, CSIS provided information that substantiated his decision. However, the Committee subsequently learned that the Service did not comply with the requirement to immediately inform the Minister afterwards. When the Minister was eventually informed about the operation—some eight months after the event—CSIS gave the reasons for the administrative error and informed the Office of the Inspector General.

One Minister-approved operation which occurred during the audit period was a cause for concern. The investigation involved the activities of a foreign power and persons working specifically on its

behalf in Canada. While the preponderance of the targeting and reporting was entirely legitimate, our review showed that the Service collected and retained information that extended beyond the original targeting authority. It is the Committee's view that the reporting was unwarranted and not in accord with current policy or the principles which have governed investigations at post-secondary institutions since 1963.

The Service collected and retained information that extended beyond the original targeting authority.

Conclusions and Recommendations

Two recommendations emerged from our study of CSIS campus operations:

> First, when requesting authorization from the Minister, the Service should be required to explain how a particular investigation will impact on the rights and freedoms of persons who are subjects of the investigation as well as those persons associated with the institution concerned.

The Service has acknowledged this lacuna and has stated that it will prepare new policy to address the issue.

> Second, the CSIS policy manual should include in the authorities section explicit reference to the 1971 Record of Cabinet Decision articulating the general principles of the Pearson-Laskin Accord on campus investigations.

CSIS saw no need for this in view of the changes after 1963 to legislation, Ministerial Direction, and Service policies.

CSIS Cooperation with the RCMP - Part II

Report #108

Among the most important of the Committee's responsibilities is the requirement to examine all agreements concluded by CSIS with other agencies and to monitor any exchange of information and intelligence they might entail. It is with respect to this part of the Committee's mandate that we present the results of the second of a two-part inquiry into relations between the Service and the RCMP.

Concentrating on the cooperative relationship at the headquarters level, Part I of the study was included in SIRC's 1997-1998 annual audit. Our goal in that review was to identify systemic problems in the relationship that would impact on the ability of either agency to fulfill the responsibilities assigned to it in the relevant governing legislation and in the principal instrument where the nature of the cooperative arrangement is articulated—the Memorandum of Understanding.

In Part I, the Committee identified several problem areas which we believed had the potential to adversely impact on the Service's effectiveness. We stated at the time, however, that a well-grounded assessment as to their significance and seriousness could not be made without examining the operational relationship in some detail. Part II, therefore, was directed principally at contacts and cooperation between the Service's regional offices and the corresponding RCMP geographical divisions.

Our specific purpose was to evaluate how

well the CSIS-RCMP arrangement was working at the regional and operational level, determine the extent to which problems identified earlier represented a potential impairment to the operations of either agency, and, if possible, suggest ways to correct or minimize them.

Methodology of the Audit

After reviewing selected files and data provided by the six regional offices of CSIS, including records of information exchanges with their counterpart RCMP divisions over the period June 1997 through March 1998, we selected three CSIS regional offices for further study.

In addition to examining all files and other documentation (hard copy and electronic) relevant to exchanges of information between the two agencies, SIRC researchers conducted extensive interviews with representatives of the Service and the RCMP. The opinions and judgements reflected in these interviews were of considerable importance in helping the Committee gain a proper understanding of the RCMP-CSIS relationship. Also necessary for this deeper understanding was consideration of events before and after the formal review period.

Findings of the Committee

Protection of Sources vs. Criminal Prosecution: an Enduring Dilemma

The mainstay of the operational relationship between the two agencies is the exchange of information via liaison officers in CSIS regions and RCMP divisions. While this part of the information exchange mechanism appeared to be working well in achieving its basic goal—providing each side initial access to key information and intelligence produced by the other body—the effective use of the information in certain situations appears to some within the RCMP to be more problematic.

Among the RCMP officials we interviewed there was a general sense of dissatisfaction about the restrictions imposed by the Service on the disclosure and subsequent use by the RCMP of CSIS-generated information and intelligence. Most seemed to realize, however, that the restrictions flowed from the legal requirements for discovery and disclosure inherent in criminal proceedings and, in particular, the *Stinchcombe* decision.

Some tension between the two agencies over the handling of CSIS-generated information is inevitable given the differing requirements and mandates of the two agencies.

As discussed in Part I of the study, some tension between the two agencies over the handling of CSIS-generated information is inevitable given the differing requirements and mandates of the two agencies. The Service exists to collect intelligence on threats to Canada using sources and methods that must be protected if they are to continue to be effective. On the other hand, the RCMP is an enforcement agency which like the Crown prosecutor, is obligated to disclose information to the Courts in support of formal judicial proceedings. In short, the Service is content to provide sensitive intelligence to the RCMP on the condition it does not reveal the information or its source. At the same time, the RCMP may need to disclose the nature of the information if it is to effectively pursue criminal prosecution and in some situations can be legally compelled to do so.

As we had anticipated upon the conclusion

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

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

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

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

of Part I of our inquiry, this ongoing dilemma has resulted in a number of localized difficulties that are the cause of some concern. In the opinion of some officers at one location, RCMP requests for the disclosure of CSIS information had declined significantly because successful prosecution could have been imperilled by legal challenges involved with using CSIS information. In the Committee's view, such an attitude to requests for disclosure cannot fail to have a detrimental effect on the operations of both agencies. The RCMP has assured us, however, that nationally the number of requests for disclosure has been relatively constant. There is no obvious solution to this conundrum within the existing Memorandum of Understanding or under existing legislation. While the potential impact of changing the law is open to debate, what is not in doubt in our opinion is the potential for damage to national security operations should the situation be left unchanged.

RCMP Liaison Officers and Alternative Information Channels

Our audit of the cooperative relationship at the regional level revealed problems in the manner in which CSIS information is provided to the RCMP. The records of exchanges show that a considerable volume of information is provided directly to functional commands

in the RCMP. The effect is to leave some RCMP liaison officers with an incomplete picture of what has or has not been provided. While the nature of RCMP arrangements to handle and process incoming information is outside the Committee's mandate, we believe that the current system could negatively influence future cooperation with the Service. We are also aware that the RCMP is seized with the problem and is studying appropriate solutions.

Overlap of Responsibilities at International Airports

The Federal Government recently transferred jurisdiction for policing at Canada's international airports from the RCMP to local police forces. A Federal policing presence was to remain, however, through the creation of RCMP Airport detachments drawn from the National Security Investigation Section (NSIS), a branch of the Force responsible for the investigation of activities described in the *Security Offences Act*.

At the outset of our inquiry there appeared to be the potential for overlap between this new organization and that of the Service which also has a presence at ports of entry—mainly in the role of assisting Citizenship and Immigration Canada in immigration security screening. (See page 9 of the 1997-98 SIRC Annual Report for a description of CSIS role in immigration.) While we found that the presence of the RCMP units at the airports created some initial confusion among other enforcement agencies as to respective mandates and responsibilities, these were quickly dispelled and have resulted in no serious difficulties.

Transnational Criminal Activity

Commencing in 1996, the Service undertook to investigate transnational criminal activity on the basis that the huge financial resources generated by international money-laundering and other illegal enterprises constituted a threat to the social and economic security of Canada. To ensure that the Service's activities were consistent with its mandate, however, its investigations were restricted, as a matter of policy, to the collection of "strategic" intelligence. The Service was to avoid involvement in individual criminal investigations.

In Part I of our review, the Committee noted that these limitations were not fully understood by some members of the RCMP who had expectations about the level of Service involvement that the Service was not prepared to meet. Our Part II inquiries at the regional and operational levels show that the misconception about the Service's role in transnational crime is ongoing.

Our inquiries at the regional and operational levels show that the misconception about the Service's role in transnational crime is ongoing.

It was evident to the Committee that the volume of relevant intelligence provided to the RCMP was relatively small. We were advised that there had been scrupulous adherence to the policy of restricting investigations to the strategic level. However, on the part of the RCMP officials concerned, the notion of "strategic" versus "tactical" investigations was still not clearly understood, and skepticism was expressed about the distinction having any validity. Several RCMP officials maintained that CSIS was withholding intelligence on transnational criminal activity from them—an accusation Service officers strenuously denied. We saw no evidence that intelligence was deliberately withheld from the RCMP. We address the

matter further in our report on Transnational Criminal Activity on page 5.

Perhaps more serious was the fact that some RCMP officials regarded the CSIS material with the same suspicion as other shared CSIS information and were reluctant to request disclosure for the same reasons. It is the Committee's view that these problems have the potential to impair Canada's efforts to control this most invidious form of organized crime. We urge the Service, the RCMP, and the Government to take appropriate action to prevent future misunderstandings.

The CSIS-RCMP relationship can be characterized as one of genuine and fruitful cooperation.

The Quality of the Overall Working Relationship

The complaints SIRC researchers heard from the RCMP officials in all three divisions they visited were for the most part directed at Service policies or the wider administrative system which they saw as creating unnecessary difficulties. The Committee heard no specific complaints about officials of the Service. A number of RCMP officials were complimentary about the Service's overall contribution to joint operations and investigations, and to the level of cooperation generally. Meetings and familiarization sessions involving both agencies were frequent (mainly initiated by CSIS officials) and there was an ongoing informal process by which issues local to the region or division were usually resolved through personal contact between senior managers from both agencies.

There continues to be some residual friction in two regions over especially difficult cases that arose in the recent past. However, the Committee believes that there has been no ongoing impairment to operational effectiveness. It is the Committee's view that with the exception of the two concerns set out above—RCMP use of CSIS intelligence in criminal proceedings, and CSIS responsibility in the area of transnational crime—the CSIS-RCMP relationship can be characterized as one of genuine and fruitful cooperation.

CSIS Liaison with Foreign Agencies

Report #112

Methodology of the Audit

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

This year, we audited two posts that have witnessed significant political and economic changes in their areas of responsibility, and which are instrumental in the collection of information on regional conflicts and terrorism. The posts examined cover a heterogeneous range of countries, most of which are developing nations. Although a few adhere to democratic principles of government, political instability is a characteristic common to most of the countries concerned, and many can be found on the watch lists of human rights observers.

The review encompassed three main categories of material:

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

The essential goals of the review were to ensure that relationships and contacts with the foreign agencies concerned corresponded to the specific liaison agreements in place, and that information disclosed to foreign agencies or received from them was properly handled by the Service. Throughout, the Committee paid particular attention to information exchanges with agencies of countries suspected of human rights abuses.

Foreign Liaison Program

For the period under review, there were no major changes to the organization of the Foreign Liaison and Visits Branch (FLV) in the wake of its establishment as a "stand-alone" branch in mid-1997. However, several management issues came to our attention.

The "Third-Party" Rule for Information Requests

It is matter of general CSIS policy on the transfer of intelligence information that foreign agencies should not be acting on behalf of other agencies (domestic or international) when making information requests. It is essential to the transparency and integrity of the dissemination process that CSIS know where information is going and who is asking for it.

Our review did identify several instances where the intelligence service of an allied country offered to act as a "broker" with agencies in other countries for information that CSIS was seeking. The Service did not accept these offers. Of a more serious nature, we learned of an instance where CSIS information was made available by the allied foreign agency to another intelligence service without permission from CSIS—an unambiguous violation of the "third-party" rule. The records show that CSIS Headquarters took a dim view of the practice and advised its SLOs to make clear to the foreign agency that it should cease these activities.

It is matter of general CSIS policy on the transfer of intelligence information that foreign agencies should not be acting on behalf of other agencies.

Yearly Reviews of Overseas Posts

In October 1996, the then manager of the Service's foreign liaison program stated that he intended to conduct a yearly review of selected foreign liaison posts to aid the formulation of recommendations for improvements to Service executives. The Committee concurred in this decision.

Since then, however, we have determined that no formal plan has been implemented. While the current Director General of the Branch continues to inspect posts on a case-by-case basis as needed, we are of the view that the original proposal for a formal and regular reporting process has advantages over the current approach. The Service holds the view that the current monitoring process is adequate.

The establishment of liaison arrangements with foreign intelligence services must be approved by the Solicitor General.

A Revised Role for Security Liaison Officers

In previous audit reports, the Committee had supported a plan to give an active role to SLOs in the process by which information to be disseminated to foreign agencies was reviewed. Under this plan, Security Liaison Officers were to act, in effect, as a last check on the appropriateness of transmitting items of intelligence to other services. We were pleased to learn that the FLV Branch has made the plan operational.

Under the new policy, a Security Liaison Officer who disagrees with the proposed release of information to a foreign agency by the relevant CSIS operational branch can seek the assistance of the Headquarters FLV Branch in order to resolve the issue. The revised policy effectively revives a management function abandoned when the former Foreign Liaison Branch was disbanded in the early 1990s.

Foreign Liaison Arrangements

Foreign liaison is governed by individual arrangements under section 17 of the *CSIS Act* between the Service and foreign intelligence services, and by a 1982 Ministerial Direction. The Direction covers contacts and exchanges by Security Liaison Officers abroad as well as visits by CSIS or allied service personnel.

The 1982 Ministerial Direction on foreign liaison states that CSIS cooperation with a foreign agency must be compatible with Canada's foreign policy. Further, the establishment of liaison arrangements with foreign intelligence services must be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade.

A Comprehensive Review of All Arrangements

In recent years, the Committee has devoted considerable attention to the Service's foreign arrangements. *Inter alia*, the Committee has identified SLO reports that favourably rated disreputable and discredited agencies, and highlighted arrangements that had been left dormant for many years. In the most recent audit report (1997-98), we noted that fully one-half of the Service's 215 foreign arrangements managed by Service SLOs posted abroad were entered into by the Security Service prior to the establishment of CSIS and, of these, many pre-dated even the 1982 Ministerial Direction.

With respect to an anticipated Government review of the arrangements as a whole we stated in 1998: "The imminent release of new Ministerial Direction will ... provide the opportunity to ensure that all foreign arrangements, particularly those that pre-date the Service, are reassessed and annotated." In furtherance of that end, the Committee also recommended that CSIS systematically reexamine all foreign arrangements following the release of the new Direction. However, as of August 1999 no new Ministerial Direction had been issued.

The Review Committee is concerned at this delay. The existing Ministerial Direction governing foreign arrangements is sadly out of date and a long-overdue comprehensive review of the arrangements is contingent on

the issuance of revised Direction. We strongly urge the Ministry to replace the 1982 Ministerial Direction with one that reflects the Government's experience with the administration of foreign liaison arrangements to date, and that is consistent with the *CSIS Act*.

New Foreign Initiatives

In the period under review, CSIS has been involved in a number of new initiatives which broaden the range of activities arising from its foreign arrangements. The Service established an intelligence training program for foreign agency personnel. The course provides instruction in intelligence analysis and insight into intelligence agency functions within democratic civil institutions. In addition, the Service rendered assistance to several foreign agencies seeking information about the drafting of legislation that would govern intelligence operations in their home countries.

Human Rights in Several Foreign Agency Relationships

Given the past records of some of the foreign agencies under the purview of the posts we examined, the issue of human rights took on even greater importance in our reviews. At one post, the only agency where an agreement was in place to exchange security intelligence information (as distinct from other, less sensitive materials) has had a poor human rights record. SIRC staff paid special attention to the information exchanges between that agency and CSIS, however, none of the information exchanged gave rise to concerns.

A foreign arrangement with a second agency, though more limited in the nature of the information that could be passed, also drew the Committee's attention. Our concern was not with the agency directly, but rather with the potential for information to find its way to counterparts in the military and the police sectors.

The Service holds a relatively sanguine view of such exchanges, maintaining that most intelligence agencies are without enforcement powers and so are less often human rights offenders. While the Committee acknowledges this point, we believe continued caution is in order. CSIS may give information to an agency that does not violate human rights, however, that agency could in turn pass the data on to other organizations of government that do. In the case at hand, we saw no problematic information exchanges from CSIS to the foreign agency.

The existing Ministerial Direction governing foreign arrangements is sadly out of date.

With respect to a third agency with a poor human rights record, we took special care to examine the exchanges of correspondence. The Committee noted that the Service was fully cognizant of the allegations of corruption, incompetence, and human rights abuses, and that it had taken this knowledge into account in the management of the relationship. The Service informed us that the relationship was contingent on the continued satisfactory human rights conduct of the foreign agency.

A Foreign Arrangement of Special Sensitivity

An arrangement of several years standing between the Service and a foreign intelligence service in a country with a history of major human rights abuses drew the Committee's particular attention.

The Service informed us that the relationship was contingent on the continued satisfactory human rights conduct of the foreign agency.

Approved by the Solicitor General, the arrangement was quite limited in scope. Incorporated into the terms of the arrangement was the provision that after a relatively short period, the agreement would be reviewed. In addition, in order to protect nationals from the government of the state concerned, CSIS was instructed not to seek information from the foreign authorities about persons still living inside that country.

In accordance with the instructions from the Minister, CSIS reviewed the relationship and, having found it useful and beneficial to Canada, the Service asked the Minister to renew it. The Solicitor General did so, with the proviso that CSIS again review the arrangement and report one year hence. When the Committee set out to verify whether CSIS had in fact complied with the Minister's instruction for another review, we determined that it had not. We were informed by the Service that they believed the instruction had been given in error.

Following consultation with the Ministry of the Solicitor General, the Committee determined that notwithstanding the Service's interpretation, the Minister's instruction was both clear and valid. The Service was obliged to review the arrangement and return to the Minister for approval. The Service has since informed us that it has written to the Solicitor General seeking approval for the arrangement.

A General Comment on Human Rights and Foreign Agencies

The essential purpose for having arrangements with foreign intelligence agencies is to allow CSIS to collect information that will protect Canadians. In the ideal world, the Service's foreign contacts would all have satisfactory human rights records—the reality is that many do not. In order to obtain the information it needs CSIS sometimes has to deal with agencies having poor human rights records.

The Committee believes that all possible care should be taken to make sure that the Service's exchanges of information are not used to assist in the violation of human rights. In order to ensure that the dissemination of information is tightly controlled, SLOs must make available to the rest of CSIS timely and accurate information about an agency's human rights record, as well as its propensity to pass information onto third parties without authorization.

Cooperation Outside the Terms of an Arrangement

Upon reviewing files detailing the information exchanged with two foreign intelligence services, we identified types of information disclosed by the Service that fell outside the limits set by the arrangements.

The disclosures took place when CSIS was informed about a plan to engage in terrorist campaigns against foreign officials. In view of the urgent nature of the information, the SLO received permission from CSIS Headquarters to disclose the information to officials of the foreign government concerned.

The Director of CSIS informed the Solicitor General of the matter. While it is clear that the disclosure of the information went beyond the scope of the liaison arrangements, Ministerial Direction gives the Director the prerogative to authorize disclosures in exceptional

circumstances. The Committee believes the Service acted properly in this case.

Dated Information

As is common practice among intelligence services, CSIS requires that its Security Liaison Officers overseas file reports on their activities and generate assessments of the agencies with which they interact. Our review of the files of one of the posts we audited revealed that key administrative reports were considerably out of date.

The importance of these reports should not be underestimated since they are a key tool enabling Headquarters staff and CSIS executives to make decisions on what should be disseminated to foreign agencies. The Committee regards this deficiency as more than a mere administrative detail. The Service has informed us that remedial actions were taken to update the files, and measures put in place to help prevent stale-dated assessments from being circulated in the future.

Dissemination to Another Agency of Government

In this instance, the Committee examined the Service's investigation of several foreign nationals who were suspected of having participated in an overseas program that threatened Canada's national security. The Service had concluded that the suspects posed no threat, yet appeared to have passed information it collected about the persons to another agency of the Canadian government. The Committee inquired of the Service about the nature of the information disseminated and the authority under which the transmission was carried out. The Service advised the Committee of the circumstances and the Committee was satisfied that the exchanges of information had been properly conducted.

A Case Under Review

A Committee review of the instructions from CSIS Headquarters to one of its SLOs seemed to indicate that an overseas officer was being asked to conduct an investigation of the kind which would have required prior Ministerial approval. No such approval had been sought and we conducted further inquiries into the issue.

Our conclusion was that CSIS Headquarters had not intended its instruction to be read as—nor did the SLO interpret it as being—a "tasking" to conduct an investigation. Instead, the apparent purpose of the Headquarters query was to make the SLO mindful of a particular situation during his discussions with other foreign representatives abroad so that any relevant information gleaned could be incorporated in ongoing updates of agency assessments.

Having informed the Service of our concern about the ambiguous communication, we noted an early response to our queries. Service Headquarters staff have since been cautioned a number of times about the need for increased diligence and precision in communications with SLOs.

A General Finding

The Committee's periodic reviews of the Service's overseas liaison activities encompass all the many difficulties associated with work in foreign posts. SLOs sometimes face environments which are personally and professionally challenging. In general, the SLOs in the two

Our review of the files of one of the posts we audited revealed that key administrative reports were considerably out of date.

posts reviewed demonstrated initiative, employed good judgement, and the Service exercised appropriate restraint in deciding what information would be shared with its foreign partners.

Areas of Special Interest - Brief Reports

Allegations by a Former CSIS Employee (S. 54)

Report #113

Under section 54 of the *CSIS Act*, the Solicitor General may at any time ask the Committee to report on a matter relating to its mandate. In July 1998, the then Solicitor General, the Honorable Andy Scott, advised the Committee of certain allegations against CSIS by a former employee of the Service. The Minister asked us to report on the matter, reviewing the allegations and detailing the facts, if any, on which the allegations were based.

The allegations were diverse in character: abuse of power, systemic abuse, nepotism, corruption, favoritism, sexual harassment, and non-compliance with the Service's policies and Canadian law. Four additional allegations concerned CSIS operations.

The Committee's research officer met with the complainant, however, he refused to provide details of his allegations on the grounds that he did not believe in the integrity of the process. Thus for details of the complainant's allegations we relied upon letters written by the complainant prior to the commencement of our inquiry.

The former employee's concerns appeared to originate in the Service's dismissal of a grievance filed in 1987. The Committee took special note of a letter sent subsequently to the Director of CSIS in which the complainant stated that if the grievance were to be settled in his favour, the additional allegations—even the most serious ones—could be somehow resolved. However, if a settlement of the grievance in his favour was not forthcoming, he would resort to using other information in his possession that would in his words "take care of the Director's hesitations."

Notwithstanding the Committee's view of this statement—effectively an attempt at blackmail—we took all of the complainant's allegations seriously and investigated each one.

In its report, the Committee took care to note to the Minister that with respect to the human resource elements of the inquiry, we were fully aware that the Service's personnel management policies lay outside the Committee's normal powers of review and investigation. Nevertheless, we were able to reach some very clear findings.

Overall, we concluded that the allegations were unfounded. The salient findings of our report to the Minister are presented below:

- Contrary to the former employee's claims that many CSIS positions were staffed on a non-competitive basis, our study determined that in fact very few were

filled by appointment, and none of those who occupied such positions had previously been employed as executive assistants as alleged by the complainant.

- We reviewed the staffing strategy as outlined in the Service's human resources policy manual. After examining all available background documents, candidate qualifications, and hiring procedures we concluded that an allegation concerning a 1997 competition in Montréal was completely unfounded. All personnel practices in this case were consistent with the established policies.

- In respect of the complainant's allegations of sexual harassment involving classes of new CSIS recruits, the Committee concluded that they too were not supported by the facts.

- The complainant made an allegation about the Service's response to a harassment complaint against one of its managers. Our review turned up no inappropriate actions in the way CSIS dealt with the complaint.

- On the issue of the Service's mandatory mobility clause for intelligence officers, we believe (unlike the complainant) the policy to be essential both for operational and professional development purposes. It would be difficult to imagine the viability of a national intelligence agency in the absence of such a personnel management policy.

- We were particularly concerned by the complainant's allegation that operational information had been collected during the course of security screening interviews for Citizenship and Immigration Canada. As noted in earlier audit reports, such allegations touch one of the Committee's special concerns. Unfortunately, this allegation was very broad and came to us unsupported by examples or details. While the paucity of details left the Committee with little to investigate in this instance, we are reassured by the fact that we routinely examine the context and content of reports following screening interviews, and that we are able to investigate thoroughly when detailed complaints are made.

- The Committee's report to the Minister also took issue with the former employee's highly tendentious view of one of the Service's former directors. We were especially disturbed by the cavalier manner in which the reliability and loyalty of a work colleague with a very impressive track record in Government service in Canada and abroad was called into question by the former employee.

- And finally, with respect to one of the more serious allegations concerning operational matters, the Committee determined that a claim that a CSIS director had deliberately concealed information from review agencies (SIRC and the Inspector General) reviewing the Service's role in the 1992 Iranian embassy attack was entirely unfounded.

- All the other allegations of an operational nature were found to be without merit.

We were especially disturbed by the cavalier manner in which the reliability and loyalty of a work colleague...was called into question by the former employee.

Although we found CSIS' file review process to be sound, we did find problems in the Service's implementation of that process.

Overlooked Files

Report #116

In early 1998, while conducting file reviews at CSIS Headquarters, the Committee came across files that were opened by the RCMP Security Service, and which had been overlooked during the Service's major review in 1990 of all of the files inherited from the RCMP. These files were still considered "active", even though their retention periods had expired and they were to have been assessed for disposal.[11]

Following our queries, CSIS conducted an internal review and found 833 files that had been missed by their review procedures. The Service concluded that a number of these files were still of operational value. We examined a sample of these files to assess the Service's rationale for retaining them.

Our review of the files revealed that the misplacing of the files was an "administrative oversight": they had inexplicably not been assigned a Bring Forward (BF) date during the Service's 1990 major review.

In general, although we found CSIS' file review process to be sound, we did find problems in the Service's implementation of that process.

Although we were informed that CSIS issued a procedures booklet in 1995, we observed that the Service's *File Review and Disposition Guidelines*, developed to assist analysts in their file disposal decisions, had not been updated since they were last amended in 1991.

> We recommend that the *File Review and Disposition Guidelines* be updated to reflect the Service's present policy and operational requirements.

The Service informed us that it would review and update its disposition procedures.

Our review showed that when the National Archives Requirements Unit (NARU) referred disposal decisions on files to the relevant operational desks, no process existed for follow-up.

> We recommend that the operational units be required to comply with NARU deadlines for disposal decisions, and that NARU establish an effective follow-up process.

CSIS said that it would establish a new BF system.

We found that the analysts' written rationales to retain files seldom referred to the specific retention criteria listed in the Guidelines. We also observed that the written rationales that were provided to support retention were not sufficiently detailed.

> We recommend that analysts in NARU and the operational desks provide detailed rationales for their decisions to retain files, citing the applicable criteria listed in the Schedules and the Service's interest pursuant to the *CSIS Act*.

Finally, in our view, a number of files should have been transferred to the National Archives of Canada, or even destroyed, because they did not appear to contain information of operational value. We have so informed the Service.

A Foreign Conflict Case

Report #106

In 1998-99, SIRC reviewed a complex and sensitive human source operation conducted over several years by the Service. Because of the high level of secrecy associated with the operation, we are constrained by national security from providing details that might put lives in danger. The Committee did find, however, that it disagreed with CSIS on significant aspects of the conduct of the operation and we have communicated our views on these difficult issues to the Director of CSIS.

SIRC View of Issue-Based Targeting

In recent years the Review Committee and others (notably the Inspector General of CSIS) have become seized with the difficulties potentially created by a form of investigation called "issue-based" targeting. This type of targeting authorizes an investigation to take place in circumstances where CSIS suspects that there is a threat to the security of Canada, but where the particular persons or groups associated with the threat have not yet been identified. In other words, the targeting authority allows CSIS to investigate the general threat, and to try to identify the persons or groups who are taking part in threat-related activities. As in any other targeting procedure, if warrant powers are involved, approval must be granted by the Federal Court.

A hypothetical case necessitating issue-based targeting could occur if, for example, a series of bombs were being exploded across the country, with no particular group claiming responsibility. CSIS would investigate under an "issue-based" targeting authority, the legal foundation for which would be the suspicion that there was a threat to the security of Canada as defined in section 2 of the *CSIS Act*.

The investigation might reveal that the bombs were the result of domestic criminal activities alone. Alternatively, it could show that a politically motivated group had decided to use violence to help achieve its political objectives. In the first case, CSIS should hand over all of its information to the police and cease its own investigation. In the second, CSIS would continue its investigation and as information became available, the investigation would be narrowed to the individuals or groups directly concerned.

The alternative to issue-based targeting in the example cited above is that CSIS would attempt to find out what was going on, and who was making and detonating explosive devices, but would do so—and this is the crucial distinction—in the complete absence of any formal targeting process and its attendant legal and administrative procedures. The differences between the two approaches might not seem very important when something as

We urge the Service to make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable.

concrete as exploding bombs is the context, but it could be most important in other less clear-cut situations.

It is the view of the Committee that issue-based authorizations are far preferable to none at all. We would take active exception to a CSIS policy that allowed any investigative activity at all to take place without an appropriate targeting authority.

While the Committee does believe that there is a place for issue-based targeting in the array of options legally available to CSIS in carrying out its responsibility to protect the safety and security of Canada, we add the caveat that investigations under such authorities should be carefully monitored by senior management. Additionally, we urge the Service to make every effort to make the transition from issue-based to individual (identity-based) targeting as expeditiously as is reasonable.

The Review Committee will continue to pay special attention to this kind of investigation so as to assure ourselves that all are being conducted appropriately.