Section 1

Review of CSIS Intelligence Activities

Review of CSIS Intelligence Activities

A. Areas of Special Interest for 2000–2001

CSIS Liaison with Foreign Agencies

Report #2000-03

BACKGROUND

As stipulated in section 38(a)(iii) of the *CSIS Act*, SIRC reviews arrangements entered into by CSIS with foreign intelligence and police agencies and monitors the flow of information to agencies with which CSIS has co-operation and information-sharing arrangements.

This year, the Committee audited a Security Liaison Officer (SLO) post overseas that operates in an especially difficult working environment. Maintaining the security of the physical operating environment is a continual, major challenge and the situation is compounded by generally onerous working conditions.

CSIS opened the post in the belief that constructive engagement through dialogue and information exchanges would assist the Service in addressing its national security mandate. The Service has sought out specific areas of common ground in which the information exchanged can serve Canadian interests and characterizes its approach to the relationship as "cautious" and "measured"—one that encourages transparency and co-operation.

METHODOLOGY OF THE AUDIT

The Committee's review encompassed three categories of material:

- all exchanges of information handled by CSIS SLOs at the post, including electronic exchanges;
- all correspondence with foreign intelligence agencies handled by the post;
- 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.

More broadly, the Committee examined the activities of the selected post in the context of the Service's overall foreign liaison program, including Ministerial Direction and the Service's policies. As it has during previous reviews of CSIS foreign liaison activities, the Committee paid special attention to any information exchanges that might potentially result in abuses of human rights by other parties.

POLICIES AND ADMINISTRATION

Foreign liaison policies are set out in Ministerial Direction. The relevant Direction, for the period under review, was issued in 1982. As prescribed by section 17 of the *CSIS Act*, the Service may enter into individual arrangements with agencies of other countries. These arrangements, which define the intended nature and scope of each co-operative relationship, are reviewed by the Committee.

Establishing liaison arrangements with foreign intelligence services must be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade. The arrangement governing exchange activities at the post selected for this year's audit was signed during the past decade.

New Ministerial Direction

As noted earlier, the Ministerial Direction relevant to the period under review was drafted in 1982. Since the Committee completed its audit of the selected SLO post, however, a new Ministerial Direction has been issued covering the entirety of CSIS operations, including foreign liaison arrangements. With particular reference to foreign liaison activities, the Committee in its 1997–1998 Report expressed concern about the need for the Government to update its Ministerial Direction and recommended that the Service re-examine all its liaison arrangements to ensure conformity with the new framework once issued. In light of these earlier comments, the Committee in its review of the new Ministerial Direction paid particular attention to those elements that pertain to foreign liaison. (For a full discussion of the new Ministerial Direction, *see* page 7.)

With respect to foreign liaison, the new Ministerial Direction appears to preserve the key policy elements of the earlier document, namely:

- arrangements are to be established as required to protect Canada's security;

- they are to be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade;
- the human rights record of the country or agency concerned is to be assessed and the assessment weighed in any decision to enter into a co-operative relationship;
- the applicable laws of Canada must be respected and the arrangement must be compatible with Canada's foreign policy.

The one significant departure from earlier Direction is that the new document grants greater discretion to the Director of CSIS to manage the individual co-operative arrangements. Formerly, Ministerial Direction gave the responsibility for setting out the specific parameters of co-operation to the Minister. The new document states that "the Director will manage these arrangements subject to any conditions imposed by the Minister."

The new document grants greater discretion to the Director of CSIS to manage individual arrangements

Since the new Direction was issued only in February 2001, it will be some time before the Committee can assess the implications of the revised policies, especially as they relate to the Director's increased discretionary authority. However, considered broadly, we believe the new Ministerial Direction is a substantial improvement over the earlier documents because the terminology employed is simpler and is consistent with that used in the legislation that governs CSIS activities as a whole.

In the Committee's 1997–1998 review of foreign liaison arrangements, and in anticipation of the new Ministerial Direction, we recommended that the Service systematically re-examine all foreign arrangements in light of the new Direction once it was issued, so as to ensure conformity. The Service has informed the Committee that it will conduct its next yearly evaluation of all liaison relationships within the framework of the new Direction.

FINDINGS AT THE POST

Overview

During the Committee's audit of the SLO post, we were struck by the substandard conditions in which Service staff were obliged to work. The poor physical facilities

at Canada's mission and an onerous workload, arising from increasingly large numbers of immigration and visa applications requiring security screening, combine to form an adverse environment. Notwithstanding these difficult circumstances, however, the SLO and staff are performing well.

We found that the SLO has made steady progress with foreign interlocutors; however, rising demands from the immigration side of the SLO's mandate left less time for developing relationships with other countries in the region for which the post is nominally responsible.

Screening Activities

The Committee's review of the post's resource allocation showed a growing share of staff time being devoted to immigration and visa security screening. In a matter of a few months the immigration/visa screening workload had risen dramatically, to the extent that additional Service personnel were temporarily detailed to the post to provide assistance. Poor physical facilities and the challenging security environment complicated matters further.

> We were struck by the substandard conditions in which Service staff were obliged to work

The evident work overload gave rise to concerns on the part of the Committee that some of the post's important functions might not be being handled expeditiously. Service senior management told the Committee that it shared our concerns and believed that the immigration workload problem extended to certain other of its SLO posts as well.

In the early 1990s, CSIS and another federal agency jointly conducted a review of the immigration-related duties at posts abroad, which resulted in more focussed use of CSIS officers' services. It is the Committee's view that the Service might wish once again to review this element of its Foreign Liaison Program. For its part, the Committee intends to conduct audits of security screening functions at selected SLO posts abroad during the course of upcoming reviews.

Information Exchanges

The Committee examined all documentation associated with operational co-operation and information exchanges involving the SLO post from March 31, 1998 through June 30, 2000. The Service's exchanges of information with the foreign agencies covered by the post were reviewed to ensure that the information disclosed to the foreign agencies or received from them was handled properly.

Our review identified only one problematic exchange. Information that tended to cast aspersions on a certain individual—but which in the Committee's view was of doubtful reliability—had been passed on to Service clients. After bringing the matter to the attention of CSIS, we were provided with additional, clarifying information. We advised the Service that it should consider giving this new information to its clients so that the earlier advice would be regarded in its proper context.

Foreign Agencies and Human Rights

Concerns about potential impacts on human rights figured significantly in the Committee's audit of this particular post. Balanced against these concerns was the basic imperative for having arrangements with foreign intelligence agencies in the first place—the need for CSIS to collect information that protects Canadians.

On several occasions in recent years the Committee has expanded on its position regarding CSIS liaison with foreign agencies. We believe the Service should take all possible care to ensure that the information it provides is not used to assist in the violation of human rights. To that end, SLOs are obligated to give the rest of the Service timely and accurate assessments of an agency's human rights record and of its propensity to pass information on to third parties without authorization. The Service must avoid situations in which it gives information to an agency that does not violate human rights, only to find that the data have been passed on to other organizations that do.

With respect to the SLO post under review, the Committee identified no information exchanges that failed to conform to these standards. It is satisfied that all human rights assessments of agencies were properly carried out.

Ministerial Direction, Revised and Updated

In February 2001, the Solicitor General issued a revised compendium of Ministerial Directions governing control and management of the Service—a development the Committee has looked forward to for some time.

THE EVOLUTION OF MINISTERIAL DIRECTION

Section 6 of the *CSIS Act* states that the Director of CSIS has the "control and management" of the Service under the direction of the Minister—specifically, the Solicitor General of Canada. The principal mechanism by which this direction is given is through written instructions or "Ministerial Direction." The Act stipulates

that the Committee be provided with copies of such directions "forthwith" after they are issued.

Ministerial Directions govern a wide spectrum of Service activities ranging from strategic policy, to guidance on specific matters such as the conduct of investigations involving sensitive institutions. In past reviews, the Committee has examined the adequacy of particular Directions, the ways in which the Service has interpreted Ministerial Directions through its own policies and procedures and how the Directions were implemented in individual cases.

Of recurrent concern to the Committee has been the disparate and patchy nature of Ministerial Directions when viewed as a whole. Over the course of the Service's 17-year history, individual ministers often issued Directions on specific matters as and when they arose. Some Directions, which are still valid as Ministerial guidance, actually predate the creation of the Service. The result has been a hodgepodge of policy guidance employing sometimes contradictory language and using terminology no longer consistent with legislation.

Ministerial guidance is streamlined, consistent in its use of language and presented in a cohesive document

NEW DIRECTION: AN OVERVIEW

The new compendium (a classified document), which replaces the old Direction in its entirety, goes a long way to rationalizing the Government's strategic guidance of the Service and, in the Committee's view, reflects a maturation of the legal and policy framework that governs the Service's work. Ministerial guidance is now considerably streamlined, consistent in its use of language and presented in a concise and cohesive document.

It is too soon to assess the effect of the revised Directions on the Service's operations. However, the compendium's relative brevity and the strategic nature of the direction given suggests that there will be an increased focus on the Service's own Operational Policies as the source for specific instructions and guidelines for implementation. Also apparent is an overall shift in discretionary powers from the Office of the Solicitor General to the Director of CSIS, with respect to the day-to-day management of the Service. In the course of future audits, the Committee intends to pay particular attention to how the new guidance is interpreted and implemented across the range of CSIS activities.

Domestic Exchanges of Information (5)

Report #2000-01

BACKGROUND

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. Section 17 of the *CSIS Act* sets out the Service's mandate to enter into these arrangements. Section 19(2) of the Act allows CSIS to disclose information to various domestic departments and agencies "for the purposes of the performance of its duties and functions."

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

AUDIT SCOPE AND METHODOLOGY

The Committee examined all Service exchanges of information, including incidental disclosures, with other domestic agencies for the fiscal year 1999–2000. In addition, the Committee conducted an on-site review of information exchange practices in one Service regional office.

The purpose of the review was to determine whether the Service exchanged information with domestic bodies in conformity with Ministerial Direction, existing Memoranda of Understanding (MOU) with government institutions and police services, CSIS operational policies, the *CSIS Act* and other relevant statutes. In particular, the Committee's enquiries sought to determine if:

- the threat necessitating the exchange sufficiently outweighed the public's reasonable expectation of privacy;
- 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 disclosures of information by CSIS to other bodies accorded with the limitations set out in section 19(2) of the *CSIS Act*;
- all exchanges of information were tracked in a consistent manner.

COMMITTEE FINDINGS

Overall co-operation

For the period under review, the Committee identified two information exchanges that raised concern. All others complied with the Service's mandate and conformed to existing policy. The information exchanged was reasonable and accurate and did not involve the unnecessary use of personal and sensitive information, nor did it infringe unduly on personal privacy.

Retention of unsolicited information

The two cases that drew the Committee's attention both arose from our on-site audit of a CSIS regional office and involved how information received from domestic agencies was managed.

In the first case, the Service's database holding the unsolicited material contained several items relating to individuals and organizations for which CSIS did not have targeting authorizations. We asked the Service to explain its reasons for retaining this material and were satisfied with the explanation. The Committee believes that in future, however, the rationale for retaining unsolicited information of a similar nature should be clearly set out in the relevant operational reports.

> **The Committee recommends that the purpose for retaining information under a general collection category be clearly identified in operational reports.**

The Service has since concurred with our recommendation and advised that the relevant section of operational policy will be amended accordingly.

The second case that drew our attention concerned the appropriateness of retaining certain information received from a domestic agency. The files related to the activities of a small group of minors. The Service told the Committee that it originally retained the material because it showed a propensity on the part of the group to engage in serious violence against persons or property for the purpose of achieving a political objective—a threat that lies within the Service's mandate. CSIS then decided, based on further assessment of the information, that no further action was required; however, it retained the original exchange of information.

The Committee fully recognizes the Service's responsibility to investigate information received from other bodies that appears to fall within its mandate. However, we question the need, in this case, to retain the information once the determination not to investigate further had been made. It is the Committee's view that the information should be deleted from CSIS records.

For its part, the Service reiterated its position on the validity of retaining the information in the first instance and noted that, in continuing to hold the information, it is preserving a formal record of information received and actions taken. The Service did agree to modify the operational reports to reflect the decision it ultimately made that the information warranted no further action on its part.

The Committee recommends that the service employ greater diligence in deciding whether to retain unsolicited information.

Review of Warrant Preparation

Report #2000-05

To obtain warrant powers under section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court accompanied by a sworn affidavit presenting the reasons why intrusive powers are required to investigate a particular threat to the security of Canada. Because properly prepared affidavits are key to the integrity of the process, the Committee periodically reviews a number of warrants selected from among a comprehensive list of all warrants active during the audit period.

Although it is the sole responsibility of the Federal Court to issue a warrant, and to attach whatever conditions it deems appropriate, the Committee's purposes in reviewing the Service's warrant preparation are twofold:

- to ensure that the facts presented in the affidavit are consistent with the information used as the basis for its preparation;
- to ensure that the facts, circumstances and statements of belief contained in the affidavit are presented fairly and objectively.

From among the warrants issued in 1999–2000, the Committee selected two for detailed review; one a counter terrorism target, the other relating to a counter intelligence investigation. The Committee examined all CSIS documents relating to the preparation of the warrant affidavits: working files, "facting" binders, internal messages, Target Approval and Review Committee (TARC) minutes, Requests for TARC Authorities (RTAs) and the affidavits themselves.

In each of the cases selected, the Committee found that the affidavit the Service provided to the Federal Court was factually consistent with the supporting documentation and that the facts and circumstances presented in the affidavit were fairly and objectively expressed.

REVISIONS TO WARRANT CLAUSES AND CONDITIONS

As noted in last year's Report (*SIRC Report 1999–2000*), the Service has undertaken a broad revision of warrant clauses and conditions with a view to simplifying the terminology and bringing it into line with current legislation. Some operational and administrative procedures were also modified.

CSIS has informed the Committee that this process is now complete and that all Service personnel involved either with applying for warrants or implementing them have been fully briefed. All changes reflected in subsequent warrant applications have been approved by the Federal Court of Canada.

Security Screening Briefs to Citizenship and Immigration Canada

Report #2001-02

The aim of this study was to assess the information provided by CSIS to the Minister of Citizenship and Immigration Canada (CIC) in its mandated role to assist the government's immigration monitoring program by supplying security screening services. The Committee last examined the Service's role in immigration in its 1997–1998 Report. Our review this year focussed specifically on the nature and quality of the advice CSIS gave to CIC in the form of written briefs.

METHODOLOGY OF THE AUDIT

For this review the Committee examined 16 of the Service's immigration security screening investigations selected from the 166 briefs sent by CSIS to CIC in the 1999–2000 fiscal year. The sample consisted of nine inland cases and seven overseas-based cases. The Committee reviewed the briefs sent to CIC and all supporting documents relevant to each investigation.

HOW THE SERVICE PROVIDES ADVICE

CSIS has the sole responsibility to provide security screening assessments for immigration applications originating in both Canada and the US. For immigration applications originating elsewhere, it is up to the Immigration Program Manager at the Canadian overseas mission concerned to request a Service security screening assessment. In either case, regardless of the advice CSIS gives to CIC, the final decision on any potential immigrant's admissibility rests with the Minister of Citizenship and Immigration.

A typical immigration security screening investigation begins when the Service receives a request from either a Case Processing Centre (CPC) in Canada or an

Immigration Program Manager at a Canadian mission overseas. The investigation ends when the Service provides its advice to CIC in one of four forms:

No Reportable Trace (NRT)—a report given to CIC when the Service has no adverse information on the immigration applicant.

Inadmissible Brief—advice provided when the Service has concluded, based on information available to it, that the applicant meets the criteria outlined in the security provisions of section 19 of the *Immigration Act*.

Information Brief—advice provided by CSIS that it has information that the applicant is or was involved in activities as described in the security provisions of the *Immigration Act*, but that it is of the opinion that the applicant does not fall into the class of persons deemed to be inadmissible under the Act.

Incidental Letter—provided to CIC when the Service has information that the applicant is or was involved in non-security-related activities described in section 19 of the *Immigration Act* (for example, war crimes or organized criminal activity) or any other matter of relevance to the performance of duty by the Minister of Citizenship and Immigration, as set out in section 14(b) of the *CSIS Act*.

All the Service briefs to CIC were found to be accurate and adequately supported by the information collected

FINDINGS OF THE COMMITTEE

Nature of the Service's Advice

All the Service briefs to CIC in which the Service rendered an opinion were found to be accurate and adequately supported by the information collected. We identified one instance in which the Service was unable to provide meaningful advice because it lacked sufficient information.

Overall, the Committee noted that the Service prepared more briefs for inland cases than for overseas-based cases, despite the fact that most immigration cases originate overseas. This issue will be examined in a future review.

Essential Statistics

During the year reviewed, the Service conducted 81 650 immigration security screening assessments, most of which resulted in a "No Reportable Trace" (NRT) response. The Service provided 166 briefs to CIC, 109 of which were inadmissible

briefs. The average time the Service needed to process an immigration security screening case that resulted in an information brief was 661 days. For cases generating an inadmissible brief, the average was 644 days. The Service's explanation for the turnaround times is found in Section 2: Security Screening, page 34.

Recent Developments

In the Committee's Report for 1997–1998, we voiced concerns about flaws in procedures for the security screening of refugee claimants in Canada. We expressed the view that the Service could and should play a greater role in assisting CIC's efforts in this area.

"Grounds to Suspect" "Grounds to Believe" Threats to Security and Inadmissibility in Canadian Law

The security screening assistance rendered by the Service takes the form of information sharing with CIC on matters concerning threats to the security of Canada, as defined in section 2 of the *CSIS Act*, and advice to CIC with respect to the inadmissibility classes in section 19 of the *Immigration Act*. These are separate Acts of Parliament and they contain distinct provisions—"threats to the security of Canada" and "inadmissibility to Canada"— each of which are brought to bear on immigration security issues.

An individual applying for immigration to Canada may be deemed inadmissible in accordance with criteria set out in section 19 of the *Immigration Act*. However, any individual (immigration applicant or otherwise) may also meet the criteria for being a threat to the security of Canada as defined in the *CSIS Act*.

The threshold for inadmissibility under the *Immigration Act* is higher than that for commencing an investigation under section 12 of the *CSIS Act*. To target an individual for a section 12 investigation the Service must have reasonable grounds to "suspect" that a person or a group poses a threat to the security of Canada. By contrast, for CIC to refuse admission for security reasons the Service's inadmissibility brief must help support its conclusion that there are reasonable grounds to "believe" that the applicant is a member of a class of inadmissible persons—a stricter standard to meet under the law.

In its briefs to CIC, the Service provides an assessment of an applicant's admissibility with reference to the *Immigration Act*. However, the Service's role in the process is not to provide advice on whether the applicant poses a threat to the security of Canada as defined in the *CSIS Act*.

The Committee has recently been advised that the Service and CIC have developed the "Front End Screening" program for refugee claimants in Canada. All refugee claimants would at the time of making a claim be subject to a screening process similar to that for applicants for permanent residence. The aim of the program is to prevent persons from being able to enter Canada and remain for an indefinite period of time without undergoing a security screening assessment—a significant risk under the procedures in place at the time of our earlier review.

This and other recent developments in the co-operative relationship between CSIS and CIC will be followed closely by the Committee.