SECRET

**File No.: 2800-154
(TD R503)**

REVIEW OF CSIS'S PRIVATE SECTOR RELATIONSHIPS (SIRC STUDY 2010-02)

**Security Intelligence Review Committee
February 14, 2011**

TABLE OF CONTENTS

1 INTRODUCTION

One of the most visible trends currently affecting security intelligence is the emphasis on achieving better intelligence by increasing integration and collaboration. This emphasis, in turn, places a new importance on the Service's relationships with partners, both foreign and domestic, including with law enforcement. This same emphasis also creates an incentive for the Service to develop relationships with non-traditional partners, such as the private sector.

The role of the private sector was acknowledged in the comments of former CSIS Director Jim Judd, who spoke of the addition of "new players" in security intelligence, asserting that the private sector has moved "into the field," bringing "new voices, new expertise and new opinions."[1] It is further reflected in the Government of Canada's National Security Policy (NSP), released in 2004, which identifies the need for "a co-ordinated approach with other key partners - provinces, territories, communities, the private sector and allies." [2] Nowhere is the new imperative to work closely with the private sector more visible than in the area of "critical infrastructure", where the need to protect that infrastructure requires the active participation of its private sector owners and operators.[3]

In past reviews, SIRC examined and commented on this movement towards greater cooperation and collaboration through CSIS's partnerships and outreach activities.[4] The present study focuses on the Service's relationship with the private sector and addresses issues connected to the evolving, and growing, role of the private sector in the context of national security. This is the first time that the Committee has examined this topic; as such, it is a baseline review that may inform subsequent reviews.

The review looks at the relationship between CSIS and the private sector in two ways. First, the discussion focuses on the Service's general liaison efforts vis-à-vis the private

[1] Remarks by Jim Judd, Director of CSIS, at the Global Futures Forum Conference, Vancouver, April 15, 2008.

[2] Privy Council Office, "Securing An Open Society: Canada's National Security Policy", April 2004, p. 5.

[3] This is further reinforced in the 2009 Public Safety Canada "National Strategy for Critical Infrastructure" that explicitly states that responsibility for critical infrastructure is shared by all levels of government - federal, provincial/territorial, and municipal - and the critical infrastructure "owners and operators". Public Safety Canada, "National Strategy for Critical Infrastructure", 2009, p. 3.

[4] See, as examples, "CSIS's Activities involving Fundamental Societal Institutions" (SIRC Study 2009-03) and "CSIS's Relationships with Select Domestic Front Line Partners" (SIRC Study 2009-04).

sector, the general goals of which are to raise awareness in the private sector, and in the public more broadly, about the Service and its mandate, as well as to advise certain vulnerable sectors of specific threats[5]. This section goes on to discuss how these liaison efforts also serve the Service's own information needs by allowing the Service to tap into information held by the private sector. This section concludes with a recommendation that the Service expand on the efforts of the Regions to be more strategic in engaging the private sector, by articulating a Service-wide strategy to manage its relations with the private sector.

The second section moves from the more general liaison relationships to a discussion of the possibilities and constraints of CSIS working operationally in closer partnerships with the private sector, something that would, *inter alia*, require that the Service share information much more freely than is currently the case. This discussion refers principally to critical infrastructure, an area with much potential for cooperation given the substantial convergence of national and private interests. Although CSIS is not the lead within the federal government for critical infrastructure[6],

The review concludes by finding that there are significant limitations on the extent to which CSIS is able to participate in close collaboration with the private sector on a legal and practical level. First and most significantly, the *CSIS Act*, developed in a different era with a different threat environment, expressly does not permit the sharing of intelligence with the private sector. Although operational policies have been developed to govern the sharing of information with the private sector, the policies are appropriately restrictive and provide strict parameters in which information can be disclosed. The Service also faces operational considerations - in particular the need to protect the integrity of an investigation - that deter it from sharing information with the private sector. On the other side of the equation, there is some reluctance on the part of the private sector to share proprietary information with law enforcement and government agencies, including CSIS.

That said, as will be discussed, there are a number of ways in which the Service does support the information needs of the private sector, albeit often indirectly by supporting the initiatives of other departments and agencies.

[5] As an example, CSIS's counter-intelligence activities would include an awareness component directed at sectors of the economy which are vulnerable to economic espionage.

[6] Public Safety Canada has the lead responsibility for coordinating Government of Canada efforts vis-à-vis critical infrastructure.

2 METHODOLOGY AND SCOPE

The review process focussed on CSIS interaction with representatives of specific industries from the viewpoint of two CSIS Regions – - each with a different private sector focus.

The intent was to have a sample that would permit a broad-based assessment of Service-private sector interaction. It is important to note that these cases do not represent all CSIS relationships with the private sector. CSIS has many relationships that serve a diverse range of requirements

SIRC received briefings at CSIS HQ and in the two Regions. Hard copy and electronic documentation were also examined. The review period extended from March 1, 2006 to January 1, 2010.

3 CSIS LIAISON AND AWARENESS EFFORTS

CSIS's relationships with the private sector range from the informal, with infrequent, ad hoc contacts to more formalized relationships that center around the execution of warrant powers. This first section will describe what types of general liaison relationships exist and how they are managed.

CSIS's liaison and outreach activities are conducted primarily at the regional level, by regional officers who either respond to requests for information or who initiate contact with firms or organizations in the private sector to identify opportunities for briefings. To provide a sense of the scale of these activities, Region, for example, has a dedicated Liaison Unit, staffed by that acts as a liaison between the regional operational desks and domestic partners, including the private sector.

CSIS has two main programs through which the bulk of these interactions take place: the Public Liaison and Outreach Program and the Liaison /Awareness Program. The Public Liaison and Outreach Program is a means of informing the private sector, and the public more generally, about the mandate of CSIS. These briefings, are given to a range of public and private sector organizations, including schools and private security firms, security personnel at shopping malls, and operators of public transportation systems. These briefings are intended both to sensitize the recipients to CSIS's mandate and, more importantly, to establish CSIS as a possible point of contact for the private sector, and for members of the public in the event that they have information of possible relevance to national security.

Through its Liaison/Awareness Program, CSIS delivers more targeted, albeit still general information to the private sector and other public organizations (e.g. universities) on specific threats, including cyber threats and threats posed to Canadian interests by foreign governments known to engage in espionage. This type of outreach is often used in connection with specific investigations the Regions are expected to foster communication and build awareness through partnerships with key public and private entities by educating and enabling our partners to identify what is a counterintelligence risk.

3.1 Goals and Outputs of CSIS Liaison and Awareness Efforts

The following section discusses the ways in which these liaison and outreach efforts are useful to the Service and concludes with a discussion of the need to be more strategic and focussed in managing these outreach efforts. The issue of the Service's outreach efforts to non-traditional partners examined here is closely linked to SIRC's recent review of CSIS's activities involving fundamental institutions, specifically religious institutions. This earlier study looked at the outreach program that was designed by the Service to serve as a link and concluded that if CSIS wishes to sustain its community outreach program, it must be more strategic, and clearly establish benchmarks against which the program's success can be measured.[10]

Service interactions with the private sector are important, in part because the private sector is ideally suited to provide the Service with unsolicited, but potentially valuable street-level information. Although beyond the scope of this review to examine in detail, it is worth noting that the ground rules for how private sector organizations may collect,

[10] SIRC Study, "CSIS's Activities involving Fundamental Institutions", 2009. This study also found that community engagement requires the relationship to be mutually beneficial.

use or disclose personal information are set out in the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Act stipulates that businesses must obtain the individual's consent when they collect, use or disclose personal information.

However, section 7.3 permits disclosure of personal information without "knowledge or consent" for reasons of law enforcement, national security, defence of Canada, conduct of international affairs, and where otherwise required by law.[11]

The potential benefit to the Service of establishing contact with the private sector is that contacts who observe something that is a cause for concern from a national security perspective, may alert CSIS.[12] Likewise, CSIS liaison contacts can generate new investigative leads and be a source of information important in the context of specific investigations.

[11] The *Privacy Act* is the federal legislation that sets out rules for how institutions of the federal government, including CSIS, must deal with the personal information of individuals and limits the collection, use and disclosure of personal information. Sections 4 and 5 of the *Act* govern the collection of personal information. Section 4 indicates only that any personal information collected by a federal government department or agency must relate directly to the programs or activities of the institution. With certain exceptions, section 5 requires institutions to collect personal information directly from the person concerned and that the person be informed of the purpose of the collection. However, this is not necessary under the *Act* in instances when informing the individual would "defeat the purpose, or prejudice the use for which the information was collected" as per 5(3)(b) of the *Act*. Notwithstanding CSIS's obligations under the *Privacy Act*, as will be discussed in the next section, CSIS does not as a rule share information with the private sector given extant legal, policy and operational restrictions.

[12] In the U.S., there are at least two well known examples of the private sector supplying vital information to security officials. In 2001, a flight school reported a suspicious student who later turned out to be a 9/11 co-conspirator. The student was not present for the attacks because he was already in custody, thanks in part to the actions of the flight school. In another instance, a New Jersey store employee was described as "instrumental" in preventing a terrorist attack in Fort Dix in 2006 when he alerted authorities to a customer who had requested that terrorist training footage be transferred from VHS to DVD. See Stacy Reiter Neal, "Business as Usual? Leveraging the Private Sector to Combat Terrorism" in *Perspectives of Terrorism*, Volume II, Issue 3, February 2008.

Contact with the private sector can also assist the private sector in protecting itself against threats.[14]

CSIS liaison work and relationship building are also essential with respect to securing and maintaining access to more specific information.

[14] This finding is consistent with SIRC's previous study that looked at the Liaison/Awareness Program in the context of CSIS's efforts to provide counter proliferation briefings to individuals working or studying in the private sector. In this case, the Service used the liaison program to develop contacts in relevant sectors and to sensitize individuals to the threat posed by proliferation. SIRC noted that the program succeeded in developing an ongoing dialogue with the Canadian business community about the threat posed by the proliferation of WMD (weapons of mass destruction), and intensified cooperation among industry representatives in this area. See SIRC's 2005 "Review of a Counter Proliferation Investigation –

In particular, the Committee recognizes the efforts of the liaison officers in this regard and the skill that they employ in developing and maintaining these relationships to the advantage of the Service. This is noteworthy in light of the fact that there is very little CSIS can "give" the private sector in return, a theme that will be explored in more detail in following section.

3.2 Challenges Associated with CSIS Public Liaison and Awareness Efforts

Both Region identified a general goal to liaise and establish a relationship, or at least make contact, with as many companies and organizations as possible. However, SIRC believes that there may be a need to devise ways of maximizing the return to the Service of these liaison efforts given the almost limitless number of private sector firms and organizations. Being focused is especially critical in light of the limited resources available to the Service to devote to this effort.

SIRC was told that the current, somewhat ad hoc nature of the Service's liaison efforts vis-à-vis the private sector represents a change, and that there were more coordinated efforts in the past to be targeted and strategic with respect to the private sector.

The absence of a current strategy for managing relations with the private sector was explicitly acknowledged by the Service. Despite the efforts of the Regions to fill this gap, there appears to be no or little HQ involvement in the process. As noted, Region has a dedicated Liaison Unit, but not all Regions have that same capacity. In the interests of leveraging the limited resources available for these activities, and of capitalizing on the experience already gained, SIRC would encourage an enhanced Service-wide discussion on the management of private sector relationships. To this end, **SIRC recommends that the Service expand on the efforts of the Regions by articulating a Service-wide strategy on managing its relations with the private sector.**

A more strategic approach that addresses issues of priority- and goal-setting could assist the Service in dealing with a potential problem identified by both Region: that current liaison efforts run the risk of

From SIRC's perspective, an effective strategy would involve identifying those sectors with the greatest potential to be of strategic value to the Service.

4 WORKING WITH THE PRIVATE SECTOR AS "PARTNERS"

This section takes a more detailed look at the limitations and possibilities of the Service working more closely with the private sector

The question of how the Service can, or cannot, work more closely with the private sector will be examined in the context of the protection of critical infrastructure, which has been identified as a principal security concern by the Government of Canada.[26] The government has articulated a "partnership" approach in Public Safety's "National Strategy for Critical Infrastructure". Specifically, the Strategy envisages cooperation and collaboration at different levels, with the goal of protecting critical infrastructure. Different responsibilities are assigned to various federal departments and agencies; between and among the three levels of government; and to partners outside of government. Critical infrastructure protection thus requires not just substantial interdepartmental cooperation, but also public-private collaboration. Although it is not the lead for critical infrastructure protection, CSIS is implicated in this discussion as the main collector of security intelligence.

SIRC concluded that there are real limitations for CSIS in developing true partnerships with the private sector in the context of critical infrastructure protection, and in general. In particular, the *CSIS Act* and the strict regime governing information-sharing limits the ability of the Service to work closely with the private sector. This challenge is not unique to Canada and, indeed, is something that western intelligence services in general are grappling with.[27]

[26] It should be pointed out that the discussion will not focus on one sector of critical infrastructure as there are many, each sector exhibiting unique issues and different configurations of partners involving federal, provincial, and local government bodies, as well as different private sector entities. On CSIS's website, "critical infrastructure" is defined as "physical and information technology facilities, networks and assets (e.g. energy distribution networks, communications grids, health services, essential utilities, transportation and government services) which, if disrupted or destroyed could have a serious impact on the health, safety, security and economic well-being of Canadians". Public Safety's "National Strategy for Critical Infrastructure" classifies ten sectors under the rubric of "critical infrastructure": energy and utilities; communications and information technology; finance; health care; food; water; transportation; safety; government; and manufacturing.

[27] For example, the March 2009, United Kingdom's Strategy for Countering International Terrorism, *Pursue Prevent Protect Prepare,* identifies as a challenge that "our understanding of those risks [for terrorism] will need to be shared with those responsible for [public] sites and public safety. Government will need to strike a balance between the familiar 'need to know' and the ever more important 'requirement to share'." There are

However, there are several ways in which the Service does support the private sector, often by participating in the initiatives of other departments and agencies. This is consistent with the integrated approach to counterterrorism, an approach that emphasizes bringing together the range of governmental and non-governmental organizations to address national security.

4.1 Sharing Information

The main challenge with respect to cooperation with the private sector has been accommodating the need, acknowledged by the Service as legitimate, of the owners and operators of critical infrastructure to have access to security intelligence while working within a system based on secrecy and the need to know principle.[28]

Indeed, Regions reported that there is significant demand in the private sector for CSIS intelligence. However, existing legal and operational guidelines governing information-sharing, developed before 9/11 created an impetus towards greater cooperation with a broader range of partners, limit the depth and scope of private-public collaboration. Although the private sector has demonstrated some reluctance to share proprietary information, the most substantial impediment is the fact that the *CSIS Act* does not contemplate disclosure of information collected by CSIS, to non-traditional/non-governmental partners such as the private sector.

Section 12: "Duties and Functions of Service"

Section 12 of the *CSIS Act* is the source of CSIS's authority to collect, analyse and retain information and intelligence on activities that are considered "threats to the security of Canada." It is also the basis on which the Service reports and advises the Government of Canada on its findings. Section 12 is important in this context because it

many such statements coming as well from the United States.

[28] SIRC was told that some, though not all, individuals in private sector firms understand the limits imposed on intelligence agencies in terms of sharing information.

limits the Service's"duties and functions" to reporting to and advising the Government of Canada, thereby restricting the Service's authority to report and advise individuals or organizations outside the Government of Canada, including the private sector.

Section 19: Disclosure of Intelligence to Government Actors

Section 19 of the *CSIS Act* prohibits disclosure of information obtained by the Service in the course of its investigations except for the purposes of the performance of its duties and functions under the Act, or the administration or enforcement of the *CSIS Act* or other laws. Section 19 specifies those situations where sharing information is permissible that depart from the Service's authority under Section 12. In particular, disclosures to law enforcement and to officers of the court in furtherance of an investigation or prosecution are permissible, as are disclosures to the Ministers of National Defence and International Affairs, or departmental officials, when the information is relevant to defence or international affairs. Section 19 also allows the Minister of Public Safety to authorize the Service to make disclosures to other Ministers or persons in the public service in the "public interest". The Act explicitly does not provide for the disclosure of information to the private sector.

"Special" Disclosures of Intelligence to Non-Government Officials

CSIS has developed operational policies[30] to address the different circumstances under which information or intelligence may be disclosed to the private sector and other non-traditional partners. In particular, the Service may make "special" disclosures outside the Government of Canada in instances when the disclosure is deemed essential to the "national interest". This would involve disclosing specific and detailed information to Members of Parliament and Senators who are not Ministers of the Crown; governments, elected officials and institutions of the provinces and municipalities; and individuals in the private sector.

Ministerial approval is required to disclose security information to non-traditional partners, and this reflects the seriousness with which the Service protects its information.[31] Of note, in all instances of special disclosures, the CSIS Director is required to submit a report to SIRC.

[30] Of particular relevance here is OPS-602 "Disclosure of Security Information or Intelligence".

"Selective" Disclosures of Information to Non-Government Actors

The Service may also make "selective" disclosures of information to members of the public,

Policy stipulates that

when making such disclosures,

Disclosing that you are a CSIS

employee to a member of the public

be an example of such a disclosure. Most information the Service shares with the private sector falls into the category of selective disclosures.

Despite the limitations on information-sharing, SIRC has found that the Service is committed to finding ways to share information with the private sector or other non-traditional partners in the event of an imminent threat to life. One option is to declassify the information so that it can be disseminated.

However, there are situations that are less clear.

An additional challenge to cooperation with the private sector is

Risk assessments combine an analysis of a given entity's ability and intent to carry out an attack (in general or against a specific location, system, or installation) with an assessment of the specific target's vulnerabilities. This focus on the *target* or location of a potential attack that distinguishes a risk assessment from a more conventional *threat* assessment, which focuses on the potential *sources* of a threat.[34] It is also this focus on the potential location or target that makes risk assessments attractive to the private sector.

4.2 Partial Solutions to the Limitation on Information Sharing

There are other, partial solutions to the limitation on sharing classified information that focus on sharing more unclassified information and expanding the number of private sector individuals with security clearances.

SIRC was advised that some of the Service's sharing of unclassified security information with the private sector takes place through ITAC (the Integrated Threat Assessment Centre), the integrated model for sharing and analyzing multi-source intelligence related to terrorism.

ITAC produces all-source, classified and unclassified threat assessments that are distributed to the private sector, first responders, and other federal and provincial/territorial departments and agencies. Provincial and federal institutions, including CSIS, support ITAC through their secondees. Secondees bring diverse skills and experiences to the Centre and facilitate access to information controlled by their respective organizations. This is one way, albeit indirectly, for CSIS to reach a broader public audience.

CSIS also distributes ITAC unclassified products directly to industry. ITAC products are thus an important tool for liaison staff in that they are often the only item that the Service can share with the private sector (and other non-traditional partners).[37]

The Regions and ITAC did identify the challenge of convincing private sector recipients of the value of unclassified information. Industry clients are reportedly gradually coming to understand that unclassified assessments from ITAC, having gone through an extensive vetting process, are more reliable than information from open sources. Efforts are also underway to increase the number of private sector individuals with security clearances.[39]

[37] The goal for ITAC is to have 50% of its products be unclassified. Of the ITAC assessments prepared to date, approximately 45% have been unclassified. Part of the strategy has been using unclassified, open source material.

[39] There are now more firms with individuals with security clearances. Region reported that private companies have been known to ask the Service for clearances; however, obtaining a security clearance requires that a government department or agency act as a sponsor

The Service is also able to support the information needs of the private sector by conducting security clearances for the private sector. Through the Sensitive Site Screening program, for example, the Service provides security clearances for individuals with access to sensitive locations, including, for example, international airports, and events such as the Olympics. This program also covers Canada's nuclear sites.

The Canadian Nuclear Safety Commission (CNSC) is the federal regulator of the nuclear sector and is responsible for regulating the entire life cycle of nuclear power plants and every aspect of their operation. In 2001, the CNSC imposed regulations under the *Critical Infrastructure Protection Act* that require employees having access to nuclear sites to have at least Site Access Clearances (SAC).

To put the size of the Service's contribution to the nuclear sector into perspective, for 2006/2007 and 2007/2008 combined, the Service performed approximately 27,100 clearance checks for the sector. SIRC views the Service's activities in this area as a positive development that contributes to the security of critical infrastructure in a very concrete way.

5 CONCLUSION

This was a baseline review, SIRC's first examination of the Service's relationships with the private sector. It examined generally how private sector relationships are managed by the Service and identified some of the challenges and opportunities presented by these relationships. Of particular interest are issues connected to the sharing and receiving of information to and from the private sector, since information sharing is closely connected with the core mandate of the Service - to collect intelligence on threats to Canada, some of which implicate the private sector very directly.

SIRC observed that there is a new emphasis on increasing integration and collaboration in security intelligence, and that there is a private sector component of this trend. The consensus appears to be that collaboration is both good and necessary.[44] This is consistent with SIRC's own observations with respect to the utility of developing relationships with the private sector. SIRC applauds the efforts of the Regions to be more strategic and focused with respect to engagement of the private sector and encourages the Service to go further in this regard.

SIRC will continue to examine CSIS's relationships with the private sector in upcoming reviews as, returning to the remarks of former Director Judd, the private sector has "moved into the field". As part of these reviews, SIRC will pursue, as appropriate, the issues raised in this study to enhance its understanding of the benefits and challenges of the Service's relationships with the private sector as they continue to evolve.

[44] See, for example, "Public-Private Partnerships (PPPs) for the Protection of Vulnerable Targets against Terrorist Attacks: Review of Activities and Findings", UNICRI (United Nations Interregional Crime and Justice Research Institute), (January 2009); Matthew J. Simeone, Jr., "Integrating Virtual Public-Private Partnerships into Local Law Enforcement for Enhanced Intelligence-led Policing" in *Homeland Security Affairs*, Supplement No.2 (2008); Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror", in *California Law Review*, Vol. 96 (2008); and, Office of the Director of National Intelligence, "United States Intelligence Community (IC) 100 Day Plan for Integration and Collaboration" (2004).

SUMMARY OF FINDINGS

- In particular, the Committee recognizes the efforts of the liaison officers in this regard and the skill that they employ in developing and maintaining these relationships to the advantage of the Service.
- SIRC observed that there are elements of the intelligence system that impede the development of true partnerships with the private sector in the context of critical infrastructure and in general.

SUMMARY OF RECOMMENDATION

- SIRC recommends that the Service expand on the efforts of the Regions to be more strategic and focused with respect to engagement of the private sector by articulating a Service-wide strategy on managing its relations with the private sector.