Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Public Report 2009 / 2010

25

Canada

Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

The Canadian Security Intelligence Service

The Canadian Security Intelligence Service (CSIS) is at the forefront of Canada's national security establishment. CSIS collects and analyzes information in order to provide advance warning to government departments and agencies about activities constituting threats to Canada, its interests and its allies. Such key threats include terrorism, espionage, foreign interference, the proliferation of weapons of mass destruction and cyber-tampering affecting critical infrastructure.

CSIS also works closely with its various domestic and international partners on issues linked to Canada's national security.

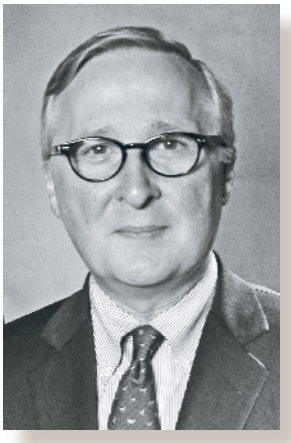
Additionally, the Service's Security Screening Program is a vital component of the Government of Canada's national security requirements and one of the most visible functions undertaken by the Service.

For more information about CSIS, please visit www.csis-scrs.gc.ca.

Table of contents

Message from the Director

The 2009-10 fiscal year has been a busy period for CSIS on many fronts, and I am proud that the Service has continued to demonstrate its value to Canadians by providing the government with crucial information and advice linked to threats to the security of Canada and its interests.



Terrorism and extremism continue to represent the most serious threat to the safety and security of Canadians at home and abroad. International terrorism is not a new phenomenon in Canada, as evidenced by the tragic bombing of Air India Flight 182 in 1985. Headlines are continually dominated by Al Qaeda or affiliates with a similar agenda and violent ideology. Canada remains the only country specifically targeted by Al Qaeda's senior leadership which has not yet been successfully attacked.

The reality of threats posed by terrorism, and in particular the domestic radicalization of extremists, has been clearly demonstrated through criminal convictions in recent years, including several members of the Toronto 18, Momin Khawaja, and Said Namouh.

While those particular threats were successfully thwarted before a terrorist attack occurred, CSIS remains vigilant about the fact that individuals or groups we do not yet know about may be planning or supporting potential terrorist plots. Domestic radicalization of extremists remains particularly concerning to intelligence services, and because there have been Canadian manifestations of the radicalization phenomenon, CSIS takes it exceptionally seriously.

Globalization has resulted in blurring of the distinction between domestic and global intelligence collection. It is rare to find any threat to Canada's security that does not have some international nexus which requires investigation, and therefore CSIS is increasing its international security intelligence operations and working closely with foreign partners.

Afghanistan and the surrounding region remain the epicentre of the Al Qaeda and Taliban core leadership, and CSIS has officers

in theatre gathering intelligence that alerts the Service to threats against Canada and Canadian personnel on the ground. The Service's specialized knowledge of intelligence-gathering has saved the lives of Canadians, Afghans and allied personnel, and has fulfilled a vitally important role in Canada's defence, diplomatic and development efforts in Afghanistan.

Terrorism is not the only threat which CSIS investigates. State-sponsored espionage against Canada is being conducted at levels equal to, or greater than those witnessed during the Cold War. Some of the same qualities that make Canada great—an open society with strong international relationships and advanced industries such as telecommunications and mining—make it attractive to foreign intelligence agencies.

CSIS is aware that certain foreign agencies are conducting intelligence operations within Canada. Similarly, foreign interference is also of concern, manifested by foreign powers that are monitoring persons or groups deemed to be of concern to their own domestic security or political agendas, gaining advantage or influencing Canadian public policy to their benefit, and perpetuating their domestic conflicts and grievances in diaspora communities overseas.

Last, but by no means least, the Service continues to dedicate significant resources to a range of other threats, from the proliferation of chemical, biological, radiological, and nuclear (CBRN) weapons, to attacks against critical information systems and infrastructure, and the sovereignty and security of Canada's Arctic territory.

During the last fiscal year, CSIS was heavily involved in security requirements for the Olympic and Paralympic Winter Games in British Columbia. The scope of the security tasks for the Winter Games went beyond that of any major event ever held in Canada, and the Service assisted its law enforcement and security partners in ensuring safe and successful Games.

On a final note I'd like to mention the people of CSIS, who on a daily basis continue to impress me with their professionalism, dedication and strong values. The Service's employee population is far

more diverse than it has ever been, and CSIS remains committed to establishing and supporting a workforce that is representative of all Canadians.

As part of CSIS's ongoing commitment to public accountability, the Service welcomes the tabling in the House of Commons of this 19th annual CSIS Public Report, which provides us with an opportunity to report on our priorities, activities and corporate issues for the 2009-2010 fiscal year.

Richard B. Fadden
Director
Canadian Security Intelligence Service

CSIS Operational Activities in 2009-2010

Operational Activities

The Threat Environment

Terrorism

Terrorism, primarily Islamist extremist violence, remains the greatest threat to the safety and security of the West, including Canadians, both within Canada and internationally. Canada is a tangible target for Islamist extremist-inspired violence.

Recent criminal convictions of individuals in Canadian courts on terrorism charges have underscored the reality of terrorist activity within Canada's borders. For example, the convictions of several individuals involved in the 2006 'Toronto 18' terrorist plot in Toronto, the case of Momin Khawaja and others illustrate the serious nature of the threat. While CSIS and its law enforcement partners successfully stopped these individuals before they acted and assisted in seeing them brought to justice, these cases clearly show that there are individuals or groups within our country that plan or support terrorist attacks to be carried out in Canada and abroad.

The threat from violent Islamist extremists now manifests itself on a number of levels. First, Al Qaeda remains the most lethal terrorist movement in the world, despite a series of setbacks and pressures in Afghanistan and Pakistan. CSIS believes that the movement continues to support the execution of acts of violence around the world. Secondly, of particular concern are those groups affiliated with Al Qaeda in one form or another that continue to train terrorists whose acquired skills could be used in future attacks. Western citizens are particularly prized by these groups for their easy access to potential targets in Europe and North America. The Al Qaeda core encourages extremist supporters worldwide to carry out attacks against Western targets.

A primary example of the amorphous nature of the Islamist extremist threat was the 'rebirth' and re-branding of Al Qaeda in the Arabian Peninsula (AQAP). Essentially a merging of the previous Al Qaeda-

related groups in Saudi Arabia and Yemen, this 'new' AQAP surprised many with its involvement in several plots in late 2009 and early 2010 in the United States. These included the infamous 'Underwear Bomber' case, where an individual believed to be working at the behest of AQAP attempted to detonate improvised explosives hidden in his underwear while on a Northwest Airlines aircraft bound from Amsterdam to Detroit on December 25, 2009.

The rapid shift in focus for the group—from being exclusively one planning attacks in Yemen to an entity with a global targeting agenda—clearly illustrated the adaptable and uncertain terrorist landscape. Additionally, the rise of U.S.-born Yemeni cleric Anwar Al Aulaqi as the world's primary English-speaking Islamist extremist ideologue showed yet again that individuals can come to the fore quickly and effectively in such terrorist groups, acting as an inspiration for many.

For its part, Al Qaeda in the Islamic Maghreb (AQIM) pursues its campaign of kidnapping and small-scale attacks in the Sahel and North African region, and appears to be a hybrid of terrorist and criminal elements. AQIM, the latest in a long line of Islamist extremist groups in the Maghreb dating back to the early 1990s, continues to show its resilience. A lesson to be learned in these cases is that removing leaders and disrupting individual terrorist cells is not enough to ensure the elimination of these groups. There is often someone else in line to assume their leadership role.

In Somalia, the previous nationalist-imbued battle by Somali Islamist extremist groups against what they perceive as being 'foreign invaders' has evolved into a local, regional and global mixture of motives and targets. Assisted by statements issued by Al Qaeda senior leaders, the Somali morass has attracted jihadists beyond the large international Somali diaspora. Many of these individuals seek to join or support terrorist groups such as Al Shabaab, a group listed as a terrorist entity under the *Criminal Code of Canada*.

The near-hopeless situation in the Horn of Africa will produce other groups wishing to use Somalia as a base for radicalization and terrorism. In particular, Canada witnessed cases in 2009 where several Somali Canadians were believed to have left this country for terrorist training camps in Somalia, demonstrating the attraction for some of travelling abroad for training and becoming ensconced within groups coordinating and planning violent 'jihad' against the West. This pattern has also been seen in the U.S. and several Western European nations.

Also of increasing concern is the phenomenon of home-grown extremists, individuals born or raised in the West who see their own countries as legitimate targets for terrorism. CSIS has actively studied the radicalization process in an attempt to understand the mindset that leads such individuals to plan or commit acts of terrorism against their own citizens and countries.

Radicalization remains a very individual process, impossible to profile with any degree of accuracy. However, several drivers do appear with some frequency, including significant grievances against Western governments, their societies or way of life. Additionally, these individuals hold a misguided belief that the Islamic world is under attack by the West, and thus needs to be defended with violence.

Persons affected by this ideology often receive such propaganda from charismatic ideologues who justify violence to achieve their goals, which in many cases are actually personal ones disguised as religious ideology. This propaganda, often promulgated through the Internet, espouses a belief that radicalized individuals are the only true practitioners of their faith. In part, this last element explains why Islamist extremists are as likely to target other Muslims, whom they accuse of not following their distorted interpretation of Islam, as they do others when planning and carrying out such attacks.

A number of factors commonly cited as important to the radicalization process are not always necessary or significant. Low socio-economic

or educational achievement, a personal experience of oppression or conflict and mental illness are not always characteristics defining the reasons why certain individuals become radicalized. In fact, violent radicals come from all social and age levels are spread widely across the educational spectrum and can appear fully integrated into society, making detection and intervention more difficult.

Also, while radicalization in prisons has not been a serious issue to date, CSIS is concerned that the incarceration of Islamist terrorists represents a potential catalyst for the types of extremist proselytizing seen in the correctional facilities of other countries such as the United Kingdom, France and the U.S. It is important to note that only a very small number of individuals have become radicalized or are of concern in this regard.

The effects of other conflicts outside Canada also continue to resonate with diaspora communities in this country. The 2009 conflict in Sri Lanka between government forces and Tamils led to mass demonstrations—and disruptions to certain local services—in Ottawa and Toronto.

Elsewhere in 2009-2010, Hizballah in Lebanon increased the pace of its Syrian and Iranian-supported military rearmament. The improved quantity, lethality and sophistication of its weapons systems have reinforced its dominance in semi-independent enclaves throughout the south of Lebanon and the Bekaa Valley, where the authority of the Lebanese Armed Forces is severely restricted. In these areas, Hizballah maintains training camps, engages in weapons smuggling and drug trafficking, and stocks thousands of rockets aimed at Israel to the south.

Additionally, by combining Palestinian nationalism and Islamist ideology, groups such as Hamas continue to call for the destruction of Israel on the one hand and a long-term ceasefire on the other. The takeover of the Gaza region by Hamas in 2007, along with its engagement in politics and competition with the Fatah, have led Hamas to

tone down some of its Islamist rhetoric by frequently placing secular political considerations before its strictly religious objectives.

On the domestic front, CSIS assesses that violence motivated by various ideologies from domestic-based groups remains a reality in Canada. Domestic extremism is motivated in part by grievances—real or perceived—and adherents to these views believe that serious acts of violence can be legitimately used as a method of bringing social attention and support to their cause, while steering government policy in their desired direction.

Eco-extremists, Aboriginal extremists and other issue-motivated groups in Canada, though very small in number, can encourage, threaten and support serious acts of violence. In certain cases, issues which provoke a sense of urgency and frustration—such as perceived policy failures or the belief that capitalism has a dehumanizing effect on society—may increase the likelihood that certain individuals or groups could adopt a more violent and destructive strategy to achieve their desired results.

Additionally, the Internet is also a central component of this, as it is used for planning, organizing and executing terrorist activities, and for recruiting participants. In fact, there are websites based in Canada that support and incite terrorist violence. The Internet and other computer-based technologies allow hostile actors to operate online in attempts to achieve their goals at a low cost, with a degree of anonymity and with a global reach.

Extremists use these resources and assets—which include email, chat rooms, instant messaging, blogs, video-sharing sites, online communities and social networks—to plan, coordinate and execute terrorist actions. They also use the Internet to conduct research on potential targets, engage in propaganda efforts, recruit supporters and personnel, solicit donations, and promote awareness of, and support for, their cause.

The cyber-related capabilities of various extremist groups have been publicly described as limited at present, but their abilities are developing and evolving. This was not a concern in the early days of CSIS as there was no broad, worldwide use of the Internet to speak of. Communication between individuals and groups that were targets or persons of interests was much more difficult than it is today and much easier for organizations such as ours to track.

But today's technologies—cell phones, satellite phones, laptops, the Internet, massive data storage drives that can fit in one's shirt pocket—are but some of the ways our targets now communicate and exchange information. Many of those who become radicalized are quite knowledgeable and capable when it comes to these new technologies and CSIS needs to keep abreast of how they are using them, and how it all functions, in order to keep track of those threats.

The varied nature of the terrorist threat—whether it is domestic-based or international in origin—requires a response on multiple levels. As such, CSIS works closely with its municipal, provincial, national and international partners to identify potential terrorist threats to Canada and its allies in an attempt to prevent such terrorist acts from occurring.

Terrorist Financing and Financial Investigation

Terrorist organizations require finances and resources to recruit and train members, distribute propaganda and carry out their attacks. Every dollar denied to terrorists makes these actions more difficult, and thus affects their ability to carry out attacks. As the activities of terrorists often have links beyond Canada's borders, CSIS receives information and consults with domestic and international counterparts on issues of mutual concern linked to terrorist financing.

In part, terrorist financing arises through fraudulent charitable fundraising, but it is often closely associated with other criminal activity including robbery, drug trafficking, extortion and kidnapping. Funds

from such activities are then siphoned through various means and used in planning and carrying out terrorist plots.

Additionally, certain investments in Canada by groups or individuals suspected of having links to terrorist groups also pose wider national security concerns. In response, amendments made last year to the *Investment Canada Act* provide the Government of Canada with a mechanism to ensure that foreign investments do not pose a threat to Canada's national security interests. CSIS plays a contributing role in the process by advising the government if a proposed foreign investment could potentially pose such a threat.

Once the Government of Canada formally lists a group as being a terrorist entity under the *Criminal Code of Canada*, all known and discovered assets in Canada are frozen, while financially and materially supporting it constitutes a criminal offence. By partnering with other agencies and institutions, CSIS remains vigilant in investigating all forms of terrorist financing or support.

Espionage and Foreign Interference

While counter-terrorism remains a priority, CSIS continues to investigate and advise the government on other threats such as espionage and foreign interference in Canadian society. Espionage is a normative aspect of global strategic and economic competition in the post-Cold War world. Canadian interests have been damaged by espionage activities through the loss of assets and leading-edge technology, leakage of confidential government information or applications, and the coercion and manipulation of ethno-cultural communities.

Foreign governments have traditionally conducted covert intelligence-gathering operations in Canada through diplomatic missions, various organizations, and by recruiting agents or informants. As a founding member of the North Atlantic Treaty Organization (NATO), a signatory to a number of other multilateral and bilateral defence agreements, and a close economic and strategic partner of the United States,

Canada remains an attractive target for espionage. A number of foreign governments continue to covertly gather political, economic and military information in this country. They have also targeted Canada's NATO allies for information related to their military and political activities within the NATO Alliance.

Globalization has compelled state actors to search for ways of remaining competitive, and to seek different methods of gaining advantage over their rivals. The rising importance of technology for sustained growth and competitiveness has made it all the more imperative for national economies to further diversify and develop their labour forces in support of economic and national security requirements. One consequence of globalization and rapid technological advances has been a noticeable increase in economic espionage, which can be defined as illegal, clandestine or coercive activity by a foreign government in order to gain unauthorized access to proprietary information or technology for economic advantage.

As a world leader in communications, biotechnology, energy extraction technologies, aerospace and other areas, Canada remains an attractive target for economic espionage. Several countries continue to engage in economic espionage against Canada, in efforts to acquire expertise, dual-use technology and other relevant information related to those sectors. Economic espionage has had ramifications for Canada, including lost jobs and a diminished competitive advantage in some fields. Canadian commercial interests abroad also continue to be vulnerable to economic espionage.

With its economic wealth and advanced infrastructure, Canada has offered attractive prospects to foreign investors. While much of the foreign investment in Canada is carried out in an open and transparent manner, a number of state-owned enterprises and private firms with close ties to their government and/or intelligence services have pursued opaque agendas. Corporate acquisitions by these entities pose potential risks related to the vulnerability of critical infrastructure, control over strategic sectors, espionage and foreign interference activities, as well as the illegal transfer of technology.

Canada has also traditionally been vulnerable to foreign interference activities. Foreign powers have engaged in covertly monitoring and intimidating various communities. In many cases, these activities are designed to support the political agendas of foreign governments, a cause linked to a "homeland conflict" or to unduly influence Government of Canada policies.

Foreign interference in Canadian society, a residual aspect of global or regional political and social conflicts, will continue to pose national security challenges to this country. CSIS will pursue its work with domestic partners and allied agencies to identify and address the threats that espionage and foreign interference pose to Canada's national interests.

Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) Weapons

The proliferation of chemical, biological, radiological, nuclear and explosive (CBRNE) weapons—also collectively referred to as weapons of mass destruction (WMD)—and their delivery vehicles (whether to states or non-state actors) poses a grave threat to the security of Canada, its allies, and to the international community. The pursuit of such weapons increases global tensions and may even precipitate armed conflicts, while their actual use in war could greatly increase levels of suffering and devastation. Canada is a party to many international conventions and other arrangements designed to stem the proliferation of WMD, and CSIS works closely with both domestic and foreign partners to uphold our country's commitment to this cause.

As noted above, Canada is a leader in many areas of high technology, some of which apply to WMD programs. As a result, Canada is targeted by foreign entities seeking to advance such programs and therefore we must remain vigilant in identifying efforts by foreign entities to illicitly obtain and use such Canadian technology, materials and expertise. This would include covert attempts by foreign govern-

ments or groups to use Canada as a transhipment point for materials destined for foreign WMD programs. Notwithstanding several positive developments such as the successful conclusion of the Nuclear Non-Proliferation Treaty (NPT) Review Conference, the Nuclear Security Summit and the negotiation of a new Strategic Arms Reduction Treaty (START) between the US and Russia, the danger of nuclear proliferation remains acute.

North Korea has tested a nuclear explosive device and is believed to have sufficient plutonium for a small arsenal of nuclear weapons. It has shown no inclination to denuclearize, as called for by the international community. Meanwhile, it is the world's greatest proliferator of ballistic missiles—including to many regions of high tension—and has proven willing to export its nuclear technology as well, as seen in the case of the Syrian nuclear reactor bombed by Israel in 2007.

Iran is also widely believed to be seeking, at a minimum, the capability to produce nuclear weapons. It has continued to advance its uranium enrichment program despite widespread international condemnation and successive UN Security Council resolutions demanding that it cease such activity.

The volatile situation regarding Iran is increasingly worrisome on several fronts and has a direct impact on national security issues for Canada and its allies. In 2009-2010, CSIS continued to investigate attempts by certain foreign governments and groups to procure WMD technology, materials and expertise within and via Canada. It also continued to seek information on the progress of foreign programs and their potential impact on national or international security, as well as on what proliferators may be seeking to acquire abroad.

Cybersecurity

Media reporting on cybersecurity issues continued to illustrate the impact of cyber-related attacks directed against the public and private sectors in a number of countries around the world. The threats

against critical information systems and infrastructure posed by foreign countries, terrorists and hackers are certainly of concern to Canada's national security and ones which CSIS continued to investigate in 2009-2010 as part of its mandate. CSIS focuses its investigations on politically motivated threats or incidents where the integrity, confidentiality or availability of the critical information infrastructure is affected. Malicious hacking activity is just one element of the threat environment which confronts Canada's national security.

Just as the Internet is global, so is the cyberthreat. Computer-based devices monitor, control and operate national critical infrastructures. Public and private sectors in Canada depend upon computer-based resources and Internet connections to facilitate their operations and their provision of goods and services to the public. However, vulnerabilities that exist within the systems and networks used by these sectors (as well as by the Canadian public in general) leave them potentially vulnerable to compromise and exploitation by a variety of hostile actors such as certain foreign states, extremists, criminals and politically motivated individuals seeking to use cyberspace for their illicit goals.

These actors pose a growing threat to national security as they target government, business, educational and private computer systems to acquire technology, intellectual property, military strategy and commercial or weapons-related information, as well as details of national strategies on a variety of domestic and foreign issues. Increasingly, cyber-related tools and techniques have been added to the methods utilized by hostile actors to attack public- and private-sector systems. State actors are openly described as using computer-based tools and techniques to exploit vulnerabilities in public- and private-sector networks, so as to further their espionage efforts directed at acquiring information and gaining access to specific targets.

Media and openly published reports note the use of botnets (networks of compromised machines that can be purchased or rented by potential attackers), crafted e-mails directed at specific targets, Twitter and other social networking services to facilitate attacks focused on stealing governmental, corporate or personal information.

These attacks use social engineering techniques to facilitate the infection of systems with malware, which allow attackers to control targeted systems, mount follow-up attacks and steal information. Some governments around the world have complained openly of cyberattacks directed against their public and private sectors, with several stating that government-backed hackers were the perpetrators. The tools and techniques used via the Internet offer a secure and low-risk means of conducting espionage and make attribution difficult.

CSIS is aware that this cyber-based variant is the fastest growing form of espionage, that the threat of cyberattacks is one of the most complicated issues affecting the public and private sectors and that attacks on the latter have grown substantially and are becoming more complex and difficult to detect. Officials and security specialists point to cyber-related threats to the critical infrastructure—which is becoming increasingly vulnerable—making specific note of the energy, financial and telecommunications sectors. Computer-related technologies, in a constant state of development and evolution, are continually being adopted by the public and private sectors. This process of evolution, development and adoption of new technologies is matched by similar processes associated with security measures and attack methodologies. This situation complicates the efforts of security and intelligence services to deal with such cyber-related threats.

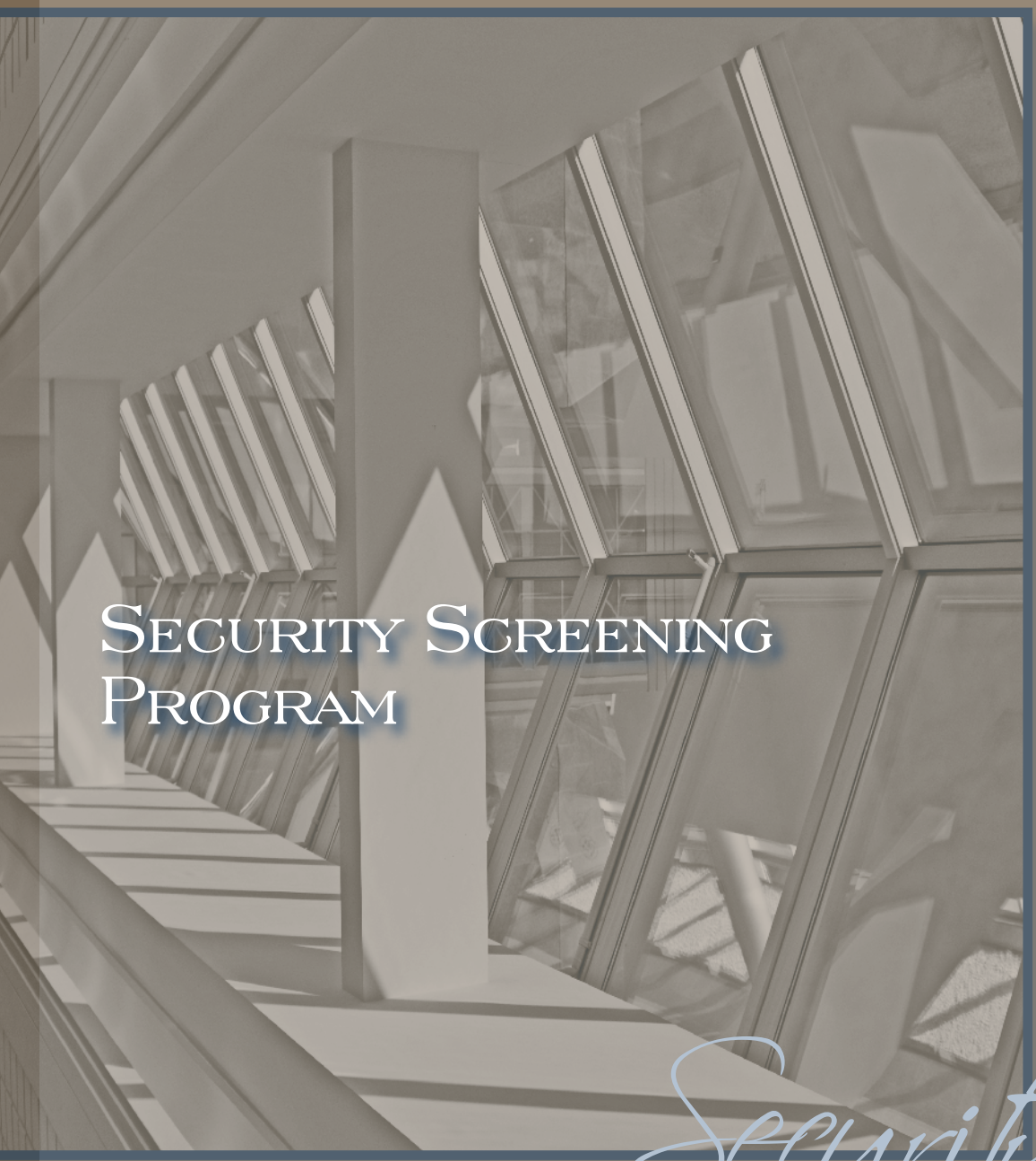
CSIS and the 2010 Olympic & Paralympic Winter Games

Olympic & Paralympic Winter Games

CSIS was heavily involved in security requirements for the XXI Olympic and Paralympic Winter Games in Vancouver and Whistler, British Columbia, in 2010. The scope of the security tasks for those events went beyond that of any major event previously held in Canada. The Service collected intelligence on possible threats to the security of the 2010 Winter Games, and CSIS fulfilled a key role on the various committees and working groups associated with the Games. The primary roles for CSIS with respect to the 2010 Winter Games were to collect, analyze and disseminate threat-related information and intelligence to support the Government of Canada in the decision-making processes during the planning, implementation and operational phases.

The common objective for the policing and security of the 2010 Winter Games was that participants, spectators, international visitors as well as Canadians remained safe and secure during this major international sporting event, while maintaining the emphasis on the Olympics as a sporting event requiring sound security measures, and not foremost as a security event with athletes. CSIS gathered intelligence on possible threats to the security of the Games through its regional, national and international partners. Furthermore, the CSIS Security Screening Branch (SSB) was responsible for the Service's role in the accreditation process and assisted the RCMP when required.

Additionally, the Integrated Threat Assessment Centre (ITAC) produced comprehensive threat assessments on a full range of terrorist and extremist threats to the Games. ITAC was designated by the Government of Canada as the lead government threat assessment centre. CSIS's efforts in this regard assisted in ensuring that the 2010 Winter Games were held in a safe and secure environment.



Security Screening Program

Security Screening

As a vital component of Canada's national security framework, the CSIS Security Screening program in 2009-2010 remained one of the most visible and primary operational responsibilities undertaken by the Service.

Government Screening

Under the Policy on Government Security (PGS), federal employees, members of the Canadian Forces or persons under contract to a government department who, in the performance of their duties, have access to classified government assets or information are required to hold security clearances. The Service assists the originating department by providing security assessments about individuals who require access to sensitive government assets, locations or information.

The PGS gives all departments exclusive authority to grant or deny security clearances. Under the authority of sections 13 and 15 of the *CSIS Act,* the Service may provide security assessments for all government departments and institutions.

Additionally, the Service's Government Screening Unit offers several site-access programs which provide assessments on individuals requiring access to major ports, airports and sensitive marine facilities, the Parliamentary Precinct, nuclear power facilities, as well as certain provincial and federal government departments. These programs enhance security and reduce the potential threat from terrorist groups and foreign governments seeking to gain access to classified information or other assets, materials and sensitive sites.

Foreign Screening

Under reciprocal screening agreements, CSIS provides security assessments to foreign governments and international organizations (such as NATO) on Canadian residents wishing to reside in another country or those being considered for positions requiring classified access in a foreign country. Canadian citizens about whom information is being provided must give their consent in advance. Screening agreements with foreign entities are all approved by the Minister of Public Safety after consultation with the Minister of Foreign Affairs.

Government Screening

Programs	Requests received *	
	2008-2009	*2009-2010*
Department of National Defence (DND)	15,300	15,000
Other departments/agencies	46,400	49,300
Parliamentary Precinct	1,000	1,100
Transport Canada (Marine & Airport programs)	36,600	34,900
Nuclear Facilities	11,100	9,500
Special Events Accreditation	16,300**	200,800**
Free and Secure Trade (FAST)	6,400	7,700
Provinces	1,000	850
Site Access - Others	2,600	3,400
Foreign checks	700	490
TOTAL	137,400	323,040

* *Figures have been rounded*
** *Increase largely due to 2010 Winter Games*

Immigration Screening

While Canada's long and valued tradition of welcoming immigrants and visitors continues, maintaining the integrity of the immigration system is a vital part of strengthening Canada's security environment. The Service's Immigration Screening Program is founded on the security-related criteria contained in the *Immigration and Refugee Protection Act* (IRPA) and the *Citizenship Act*. The Service provides advice to Citizenship and Immigration Canada (CIC) through this program in order to help it with its decisions, as well as to the Canada Border Services Agency (CBSA).

The program has the following essential screening components: visitors from countries of terrorist and espionage concern; refugee claimants in Canada; applicants for permanent residence from within Canada and abroad; and applicants for Canadian citizenship. The CSIS authority in this regard is provided under sections 14 and 15 of the *CSIS Act*.

Immigration Screening

Programs	Requests received *	
	2008-2009	*2009-2010*
Permanent Residents Within and Outside Canada	67,300	68,400
Front-end Screening	26,800	23,500
Refugee Determination Program	6,600	9,200
Citizenship Applications	169,500	175,500
Visitors Visa Vetting	58,900	67,800
TOTAL	329,100	344,400

** Figures have been rounded*

Domestic and International Cooperation

Cooperation

Cooperation with domestic and foreign organizations is absolutely essential for any intelligence service to effectively carry out its mandate. Such cooperation allows CSIS to access a much broader range of timely information, which might otherwise not be available to Canada. The Service can thus better evaluate current and future threats to our country and its interests. CSIS works with a wide variety of partners in Canada and abroad.

Domestic Cooperation

CSIS is geographically dispersed across Canada. The CSIS National Headquarters (NHQ) is located in Ottawa, and the Service also has Regional Offices in Halifax, Montreal, Ottawa, Toronto, Edmonton and Burnaby. Furthermore, CSIS has District Offices in St. John's, Fredericton, Quebec City, Niagara Falls, Windsor, Winnipeg, Regina, and Calgary. This geographic configuration allows the Service to closely liaise with its numerous federal, provincial and municipal partners on security issues of mutual interest.

Additionally, CSIS also has several Airport District Offices, including those at Toronto's Pearson International Airport and at Vancouver's International Airport. These offices support aviation security, and assist CIC and CBSA officers on potential national security issues. The CSIS Airport District Offices also provide information to their respective CSIS Regional Offices and to CSIS Headquarters, and liaise with other federal government departments and agencies that have a presence within Canada's airports.

In 2009-2010, CSIS continued to share information on security issues with a wide variety of domestic partners, and worked closely with the various Canadian government departments and agencies to ensure the collective security of Canada. A key component of CSIS cooperation with its domestic partners remains the production and dissemination of intelligence reports and assessments such as those drafted by the Service's Intelligence Assessments Branch (IAB) and Canada's Integrated Threat Assessment Centre (ITAC), which is housed within CSIS Headquarters.

Intelligence Assessments Branch (IAB)

CSIS produces intelligence assessments regarding threats to national security, as they are defined in section 2 of the *CSIS Act*, which include terrorism, espionage or sabotage and foreign-influenced activities detrimental to Canada. The CSIS Intelligence Assessments Branch (IAB) provides a range of products to the Government of Canada and certain allied foreign agencies, including concise analyses of threat-related issues and reports identifying emerging trends or threats having national security implications for Canada.

IAB analytical reports are written by subject-matter experts based on an extensive review of classified reporting, as well as open-source information. They are designed not only to explain general threat trends, but also to address more narrowly focused issues based on particular client needs.

The mandate of the IAB is to provide timely and focussed intelligence which meets the Government of Canada's stated requirements and priorities. IAB reports* disseminated to the Canadian government and to certain foreign agencies include: 'CSIS Intelligence Assessments' (IAs); 'CSIS Intelligence Reports' (CIRs); 'Foreign Agency Reports' (FARs); and 'Threat and Risk Assessments' (TRAs).

For a more detailed look at the IAB's roles and responsibilities, as well as a description of the aforementioned reports produced by the Branch, please refer to the 2008-09 CSIS Public Report.

Integrated Threat Assessment Centre (ITAC)

Canada's National Security Policy of 2004 established the Integrated Threat Assessment Centre (ITAC), whose primary objective is the production of integrated, comprehensive and timely assessments of the terrorist threat to Canadian interests, both domestically and internationally. ITAC's threat assessments are distributed within the intelligence community, to law enforcement and other first responders,

and to critical infrastructure stakeholders in the private sector. Since it became operational in October 2004, ITAC's threat coverage has been expanded to include threats to special events, all sectors of Canada's critical infrastructure, and the threat of serious violence from domestic extremism.

ITAC is a community-wide security and intelligence resource staffed by federal representatives from the following organizations: CSIS, Public Safety Canada (PS); RCMP; CBSA; DND; FINTRAC; Communications Security Establishment Canada (CSEC); Department of Foreign Affairs and International Trade (DFAIT); Privy Council Office (PCO); Transport Canada (TC); Correctional Service Canada (CSC); and Public Works and Government Services Canada (PWGSC). These representatives bring the information and expertise of their respective organizations to the Centre. The Ontario Provincial Police (OPP) and the Sûreté du Québec (SQ) also have members assigned to ITAC to act in a liaison capacity with Canada's first responders.

ITAC works under the authority of the CSIS Director, in consultation with the National Security Advisor (NSA) to the Prime Minister of Canada. ITAC receives its strategic direction, guidance and advice on requirements and priorities from the ITAC Management Board, an interdepartmental committee of Deputy Ministers from contributing departments and agencies which is co-chaired by the NSA and the Director of CSIS.

In 2009-2010, ITAC produced and disseminated more than 400 threat assessments, including numerous assessments prepared in support of security efforts for the 2010 Vancouver Olympic and Paralympic Winter Games. Internationally, ITAC cooperates with allied integrated threat assessment centres, thus providing Canada and its partners with a global perspective on the threat posed by terrorism.

Foreign Operations and Cooperation

Exchanging information with foreign agencies is an integral part of the Service's mandate. Canada's international obligations and commitment to national security create a strong presumption in favour of sharing threat-related information. Foreign terrorists inspire and provide direction to individuals and groups in Canada, while a small number of Canadian citizens are training in terrorist camps abroad or attempting to conduct terrorist operations in other countries.

Additionally, Canadians have been kidnapped in places such as Iraq, Afghanistan, Somalia, Pakistan, Niger, and the Sudan, while Canadian Forces and government officials in high-risk areas such as Afghanistan face a constant threat. Lastly, Canadian citizens travelling in other areas of the world—whether for business or personal reasons—remain at risk of being caught in a terrorist attack, as happened in Mumbai, India.

Given the current international threat environment, it is essential that CSIS maintain strong relationships with foreign agencies and continue to exchange information on potential threats to Canada and its citizens. Globalization—a loose term that alludes to such things as easy international travel and transnational interests—has resulted in a blurring of the distinction between domestic and global intelligence collection.

Consequently, the Service has increasingly focused on global issues and become more active in the international arena. Meanwhile, Canada must react to and navigate within a threat-rich and competitive environment.

In 2009-2010, CSIS implemented four new foreign arrangements and as of March 31, 2010, had 280 foreign arrangements in 148 countries. As per section 17(1)(b) of the *CSIS Act* and Ministerial Directives on 'Foreign Arrangements & Cooperation', prior to entering into such agreements, all Service foreign arrangement requests must be reviewed by the Minister of Foreign Affairs and approved by the Minister of Public Safety.

Additionally, the Security Intelligence Review Committee (SIRC) and the Inspector General (IG) carefully examine the Service's foreign arrangements and monitor the exchange of information to ensure that the terms of the arrangements are upheld.

CSIS shares information with foreign agencies on a number of issues. For security, privacy and confidentiality reasons, the Service does not publicly divulge details of that information nor identify the foreign agencies in question. CSIS must protect its foreign arrangements in order to keep such relationships viable and secure. Foreign agencies expect that the information they provide to us will be kept confidential; similarly, CSIS expects that any information it provides to foreign agencies will not be publicly divulged.

When exchanging information with foreign agencies, CSIS uses appropriate instructions or caveats which were enhanced following recommendations made by the O'Connor Commission of Inquiry. The caveats applied by CSIS to accompanying information shared with foreign agencies seek assurances that any Canadian citizen detained by a foreign government will be fairly treated within the accepted norms of international conventions. Such caveats also seek assurances that the detainee is accorded due process under law and afforded access to Canadian diplomatic personnel, if requested.

CSIS also had approximately 50 officers stationed in several countries abroad during the period under review, including in cities such as Washington, Paris and London. Their primary functions are to provide screening support to Canada's Citizenship and Immigration (CIC) offices abroad, to liaise with international partners, and to collect security intelligence information related to threats to Canada and Canadian interests.

Over the past several years, the Service has strived to improve and increase its presence and collection efforts outside of Canada's borders. In 2009-2010, the Service increased its capacity to collect quality intelligence abroad through CSIS stations and its relationships in priority areas around the globe. There have also been improved coordination and understanding of the Service's collection mandate

abroad among stakeholders within Canada. The Service's ability to utilize its relationships with foreign services and leverage their knowledge and capabilities has produced enhanced collection in response to the government's security intelligence priorities.

In 2009-2010, the Service also continued to provide increased and timely reporting from the Afghanistan and Pakistan region in support of Canada's mission in Afghanistan. It also supported allied efforts to combat extremism emanating from this volatile region of the world and contributed to save Canadian, allied and Afghan lives.

Inside CSIS

Inside

Our People

In 2009-2010, the number of full-time equivalents (FTEs) at CSIS totalled 3,104, which represents an increase of approximately 15% from the total number of FTEs at CSIS in 1993. The growth in this regard has not been as dramatic as some reports in the public domain have suggested, when one compares the scope of today's threat environment to what it was in the early 1990s.

The CSIS workforce is diverse, consisting of people from different backgrounds working in a variety of positions such as intelligence officers, analysts, surveillants, technologists, engineers, translators, corporate officers and administrative support staff. Women and men are nearly equally represented, at 49% and 51% respectively. Sixty-two percent of employees identified English as their first official language, while 38% identified French.

Additionally, 67% of the total workforce is bilingual (speaking both of Canada's official languages), while 27% speak a third language. Collectively, Service employees speak approximately 105 foreign languages. At CSIS, employees are recognized for their skills, talents and contributions. In 2009-2010, the Service continued to remain a career choice for employees as evidenced by a low resignation rate of approximately 1%.

However, like many other organizations, CSIS continues to face corporate challenges on the personnel front. For example, new CSIS recruits are increasingly required to learn their jobs much faster than in past years, largely due to increasing retirements of the 'Baby Boomer' generation. The Service must continue to keep a good balance of experience and expertise in place while recruiting and training new employees to take over from those who retire.

Employee Recruitment

Recruitment and diversity go hand-in-hand and the Service has developed the necessary infrastructure to ensure CSIS is hiring people who reflect the Canadian population. In this regard, the 2009-2010

recruitment plan for the Intelligence Officer category included a 25% target for three of the four designated groups (Aboriginals, Visible Minorities, Persons with Disabilities), as women are already well-represented in this category. During the period under review, the Service also continued its recruitment initiatives, resulting in more than 300 new hirings from across the country. Additionally, individuals considered in 'mid-career' have continued to join the organization, as demonstrated by the average age of hire (35) during the fiscal year 2009-2010.

The Service also continued to participate in career fairs sponsored by the Government of Canada and to promote CSIS and the Public Service as employers of choice. In this vein, the Service participated in more than 75 career fairs across the country in 2009-2010 and provided information sessions to a variety of different student and community groups.

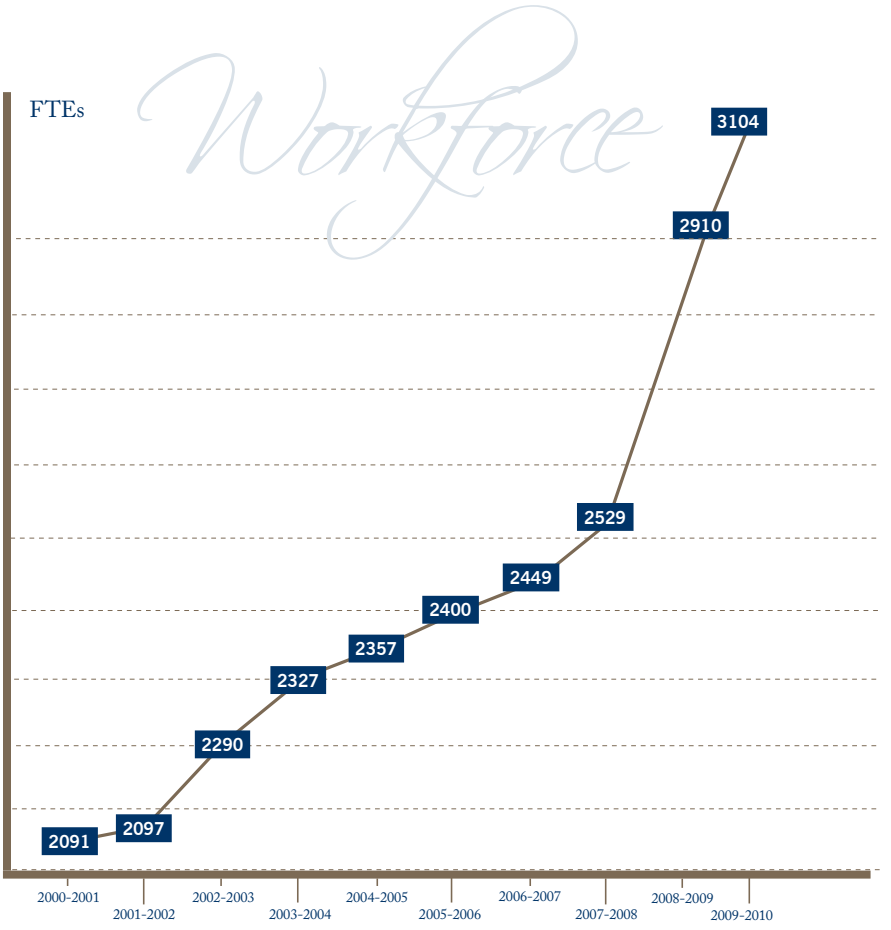
A CSIS Diversity Recruitment Officer position was implemented to focus on establishing contacts, building awareness and demystifying the role of the Service with communities across Canada, as well as at universities and colleges. Additionally, a Diversity Management Unit was created to ensure that all talent-management processes are approached with diversity in mind.

As a knowledge-based organization, the Service continued to invest in ongoing learning for all employees. The existing Entry-to-Exit training framework (an all-inclusive, career-long approach to learning) ensures that the Service's training agenda is clearly aligned with its strategic direction and priorities. Furthermore, as a career employer that values its employees, CSIS adopted new initiatives to develop and enhance the core leadership competencies of its managers.

Finally, the Service continued to strengthen its brand. For the second year in a row, CSIS made the list of Canada's 'Top 100 Employers'. It also was named as one of the National Capital Region's 'Top 25 Employers' in 2010, the third consecutive year the Service has received this honour. The Service remains committed to the principle of Public Service Renewal; CSIS's respectful and responsive workplace lends itself to productivity, innovation and management excellence.

CSIS Workforce 2009-10

No. of FTEs	3,104
% of bilingual employees (English and French)	67%
% of IOs who speak a language other than English or French	27%
Gender split	51% men / 49% women



CSIS National Headquarters

The Service's National Headquarters (NHQ) is located in Ottawa, Ontario. The Government of Canada awarded a construction contract to EllisDon Corporation for the CSIS building addition (known as Phase III) as a Major Crown Project valued at just under $69.5 million.

In March 2009, construction began on the five-storey tower expansion to the CSIS NHQ, and the project is expected to be completed in mid-2011. Public Works and Government Services Canada (PWGSC), in partnership with CSIS, coordinates the development of this project.

Profile

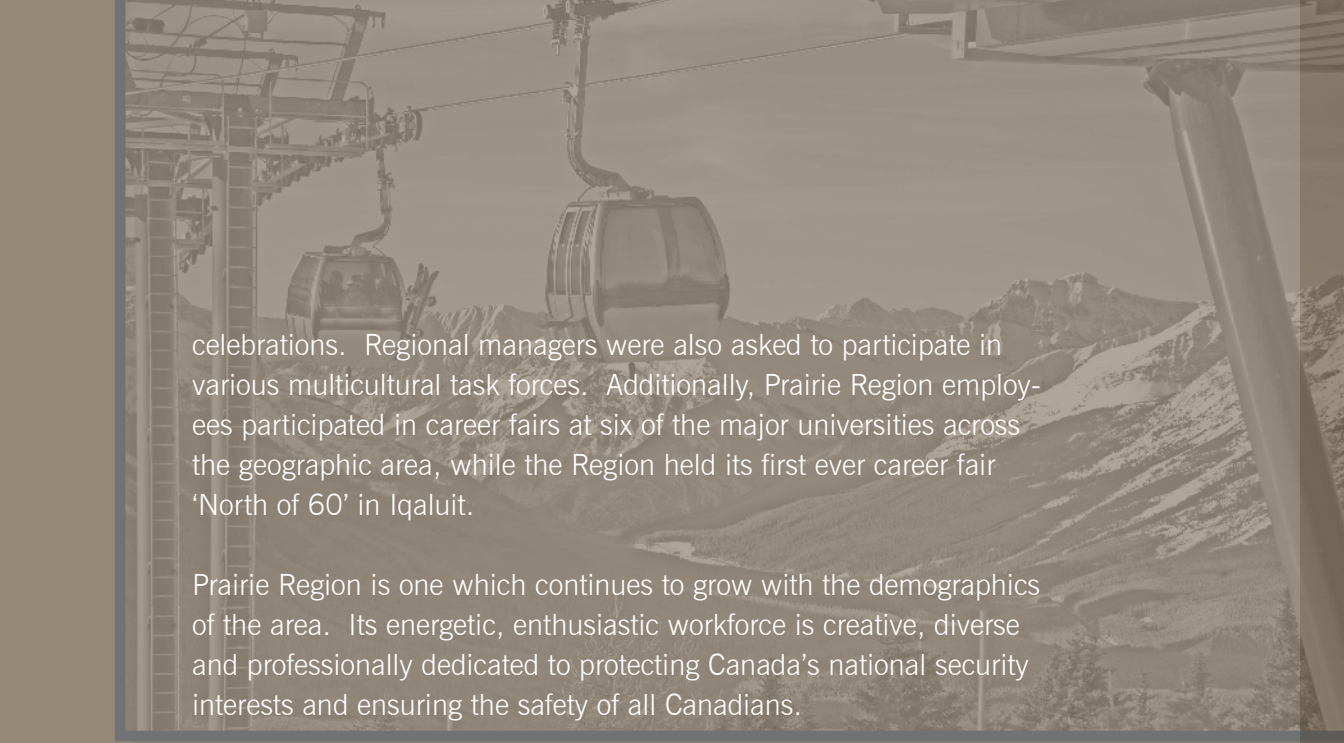
REGIONAL PROFILE: PRAIRIE REGION

Prairie Region (PR), the largest of CSIS's domestic Regions, encompasses almost two-thirds of the land mass of Canada, incorporating four provinces and three territories. The Region's area of responsibility includes the provinces of Alberta, Saskatchewan and Manitoba, northern Ontario (in the area west and north of Thunder Bay) and the northern territories of the Yukon, Northwest Territories and Nunavut. The Region is comprised of the Regional Headquarters located in Edmonton, with four District Offices situated in Calgary, Edmonton, Regina and Winnipeg.

This area of Canada, once considered the "frontier of the nation", is currently one of the fastest-growing regions of the country, both in terms of population and of economic prosperity. The economies of this region are diverse and include a vibrant oil and gas industry, robust gold, diamond, uranium and potash mining sectors, a strong agricultural base and world-class biomedical research facilities and universities. While the economies are long established in the Prairie provinces, the untold potential of the North itself is now opening up.

The thriving economies and ensuing population boom have also resulted in an increased number of people into the region who represent threats to national security. Indeed, the size and diversity of the Prairie Region pose some unique challenges. Public safety remains the primary operational priority in that Region and its resources remain fully committed to this issue.

One of the Region's major goals in 2009-2010 was to put on a public face in order to give people a greater awareness of the Region's important work. This meant that Prairie Region employees from all levels made a firm commitment to become actively engaged in a number of public and private forums. For example, Prairie Region participated in a number of community outreach programs, which resulted in many of its officers being invited to community, religious and cultural



celebrations. Regional managers were also asked to participate in various multicultural task forces. Additionally, Prairie Region employees participated in career fairs at six of the major universities across the geographic area, while the Region held its first ever career fair 'North of 60' in Iqaluit.

Prairie Region is one which continues to grow with the demographics of the area. Its energetic, enthusiastic workforce is creative, diverse and professionally dedicated to protecting Canada's national security interests and ensuring the safety of all Canadians.

Other interesting points about Prairie Region:

- The total area of the Region exceeds six million square kilometres;
- The metropolitan areas of Calgary and Edmonton both exceed one million inhabitants, while the city of Winnipeg is approaching a population of 800,000;
- Officers from Prairie Region sit on six Federal Councils and the Region also maintains active and productive liaison with seven RCMP Divisions and another nine municipal police forces;
- The area covered by Prairie Region borders six U.S. states, and all of the Region's Districts maintain strong and ongoing communications with their American federal partners;
- There are six international airports, three international marine ports and 38 recognized land crossing Ports of Entry from the United States throughout the Region's geographic area of responsibility.

CSIS Financial Resources

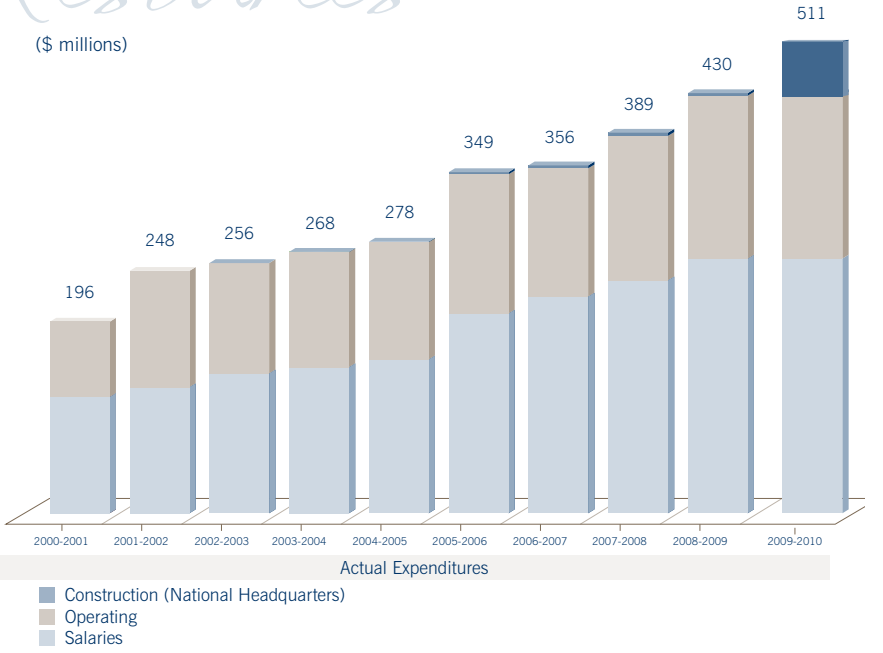
CSIS's final expenditures for 2009-2010 totalled $511 million.

The Service's financial resources have increased since 2001-2002, partly as a result of new funding for public security and anti-terrorism initiatives allocated in the December 2001 Federal Budget. In addition, CSIS received resources for its part in the Government of Canada's Marine Security Initiatives and the Canada–U.S. Smart Borders Declaration. In the past few years, additional funding was also provided to augment the Service's foreign collection capabilities, to administer Canada's Integrated Threat Assessment Centre, to help CSIS maintain its operational capacity both domestically and abroad, to expand its National Headquarters and to bolster existing capacities to combat terrorist financing.

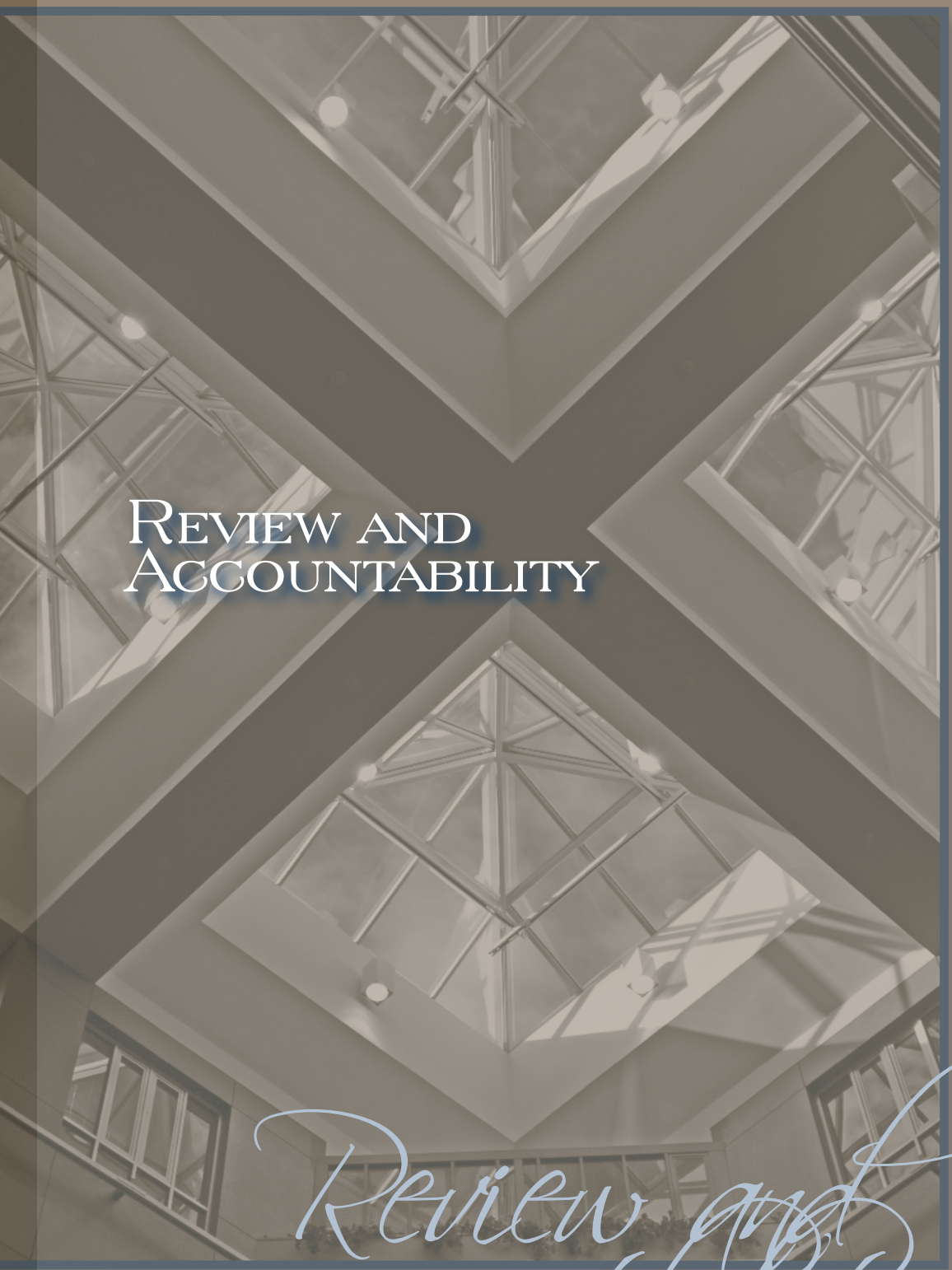
Incremental funding was approved for planning and operations related to policing and security of the 2010 Olympic and Paralympic Winter Games in Vancouver. Over a period of three fiscal years (2007-2008 to 2009-2010), CSIS received a total funding of $11 million in support of the Service's role and requirements related to the security of the Games.

Finally, CSIS was part of the Government of Canada's strategic review process in 2009-2010 so as to rationalize operations and ensure alignment with organizational needs. Total savings of $15 million were identified as part of this strategic review and approved in Budget 2010, to take effect in 2012-2013. As a result of this exercise, CSIS is better positioned to focus on high priority activities.

Resources



Construction costs shown are for the expansion of CSIS NHQ. Costs incurred from fiscal year 2002-2003 to 2006-2007 represent expenditures associated with the project definition stage. In 2007-2008 and 2008-2009, costs incurred were mainly attributable to the building's site preparation. The construction of Phase III began in the summer of 2009, with total expenditures of $44 million in 2009-2010.



Review and Accountability

Review and Accountability

CSIS is one of the most reviewed intelligence organizations in the world. Fully two-thirds of the Service's enabling legislation, the *CSIS Act*, is dedicated solely to ensuring that the Service is subject to proper reporting and accountability mechanisms. The activities of CSIS are subject to the review of the Security Intelligence Review Committee (SIRC), the Inspector General (IG) for CSIS, the Federal Court, as well as by various officers of Parliament, including the Auditor General and the Privacy Commissioner.

In practice, what this means is that the Service has had more than 25 years of experience working under ongoing review and accountability mechanisms; it is ingrained in our culture. Although we may not always agree with the findings of those who review us, it is obvious that this review system has made us a better organization. We have become accustomed to a regular review of our activities, which for us has resulted in an ongoing process of adjustment and refinement.

The CSIS Director is accountable to the Minister of Public Safety, who is responsible for providing Ministerial Direction to the CSIS Director on the policies, operations and management of the Service. The operational activities of the Service are primarily reviewed in an ongoing manner by two review bodies established by Parliament in the *CSIS Act* - SIRC and the IG.

The Security Intelligence Review Committee (SIRC)

The Security Intelligence Review Committee was established in 1984 as an independent, external review body which reports to the Parliament of Canada on Service operations. Each year, SIRC undertakes a series of reviews of operations and activities conducted by CSIS. SIRC also investigates complaints concerning the Service's activities, or the denial or revocation of a security clearance. Following each review or complaint investigation, SIRC provides its observations and recommendations pertaining to the CSIS policies, programs or operations under review. While CSIS is not required by law to implement SIRC recommendations, the Service always gives them careful consideration. In fact, most of SIRC's recommendations have been implemented by CSIS.

The SIRC Annual Report, tabled by the Minister in Parliament and available to the public, provides an unclassified overview of its various studies of CSIS issues conducted during the fiscal year, and of the results of its complaints investigations.

The Service's interactions with SIRC (and with the IG) are primarily managed by the CSIS External Review and Liaison (ER&L) Unit. This includes coordinating requests or questions relating to reviews, and providing advice to CSIS employees during reviews or briefings.

Additionally, ER&L serves as the primary liaison point regarding complaints against CSIS filed with SIRC under sections 41 and 42 of the *CSIS Act*. The ER&L Unit works with all Branches of the Service, and with its counsel, to coordinate the Service's response to the complaint. The combined efforts of SIRC and the IG over the years have made the Service a more effective and professional organization. The Service remains committed to working with its review bodies and to maintaining a productive and professional relationship with them.

The Inspector General (IG)

The mandate of the Inspector General (IG) for CSIS is to support the Minister of Public Safety in exercizing ministerial responsibility for the Service. The IG is responsible for monitoring CSIS compliance with operational policies, reviewing its operational activities, and reviewing and issuing a certificate indicating the degree of satisfaction with the Director's Annual Report on CSIS activities, which is provided to the Minister of Public Safety under section 33 of the *CSIS Act*. An unclassified version of the IG's annual certificate is available on the Office of the Inspector General's web page, via the Public Safety Canada website.

Access to Information and Privacy

During the 2009-2010 fiscal period, the CSIS ATIP Unit received a total of 301 requests under the *Privacy Act* and 156 requests under the *Access to Information Act.*

The Access to Information and Privacy (ATIP) Unit is located within the Service's Secretariat Branch. The ATIP Unit currently has an establishment of 15 employees to fulfill the Service's obligations under the *Access to Information Act* and *Privacy Act*. The CSIS ATIP Coordinator has the delegated authority from the Minister of Public Safety Canada to exercise and perform the duties of the Minister as head of the institution.

In 2009-2010, the ATIP Unit continued to conduct ATIP awareness sessions for all new CSIS employees. A number of briefing sessions were also given to managers and other specialized functional areas. Twelve sessions were given to 372 participants who were provided with an overview of the *Privacy Act* as well as the *Access to Information Act*, and a better understanding of their obligations and the process within CSIS.

The ATIP Coordinator liaises with the Treasury Board Secretariat, the Information and Privacy Commissioners and other government departments and agencies on behalf of CSIS. In addition, the ATIP Unit processes and responds to all *Privacy Act* and *Access to Information Act* requests made to CSIS.

The *Privacy Act* came into force on July 1, 1983. Under subsection 12(1) of the Act, Canadian citizens, permanent residents and individuals present in Canada have the right to access their personal information under the control of the Government of Canada. This right of access is balanced against the legitimate need to protect sensitive information and to permit the effective functioning of government while promoting transparency and accountability in government institutions.

In addition, the Act protects an individual's privacy by preventing others from accessing his or her personal information, and manages the collection, retention, use and disclosure of personal information.

CSIS Internal Audit Branch

The Internal Audit function at CSIS is headed by the Chief Audit Executive (CAE), who reports to the CSIS Director and to the Audit Committee. The CAE provides the Director, Senior Management and the Audit Committee with independent, objective advice, guidance and risk assurance on the Service's risk management strategies and practices, management control frameworks, systems and practices, and governance processes.

In July 2009, the amended Treasury Board of Canada Secretariat (TBS) Policy on Internal Audit took effect. The new policy prompted a review of the Service's Internal Audit Policy, Internal Audit Charter, and Audit Committee Charter. This policy set was subsequently revised to reflect TBS emphasis on Audit Committee advisory responsibilities.

CSIS Audit Committee membership remained stable throughout 2009-2010, with three external members and four ex-officio members from the CSIS senior management team. In its second full year, the Audit Committee continued to contribute to the quantity and quality of attention accorded within CSIS not only to the internal audit function, but also to the core areas of management, control and accountability. The Audit Committee concluded that CSIS had made significant progress in all five areas of principal interest to the Committee – risk management, management control framework, financial reporting, values and ethics, and the internal audit function.

Business Modernization Project

In June 2009, CSIS undertook a thorough review of the Service's business practices and operations, with a view to modernizing the organization following its 25th anniversary. The objective of the review was to conduct a thorough study of how CSIS currently operates at all levels, to systematically and scientifically map how it conducts its business, and to determine best practices and efficiencies to make the Service better than it has been over the past quarter century.

The review was given the title of 'Business Modernization Project' (BMP) and a small team of individuals was assigned to conduct the review and begin the assessment process in September 2009. The team included both CSIS operational personnel and Service individuals with a background in business process issues, in order to provide a profound understanding of how CSIS would approach the project and what was needed to bring it to fruition.

The BMP team subsequently shared its findings and initial recommendations to the CSIS Director and Executive members. Its final report, which includes the detailed recommendations and an implementation strategy, was presented to the CSIS Executive Committee in July 2010.

The most noticeable change is the creation of a new organizational structure, with the aim of increasing operational capacity, consolidating and enhancing analysis and production functions, and enhancing corporate support.

Improving Current Practices

In November 2009, a 'Working Group on Unexplored Operational Investigation Initiatives' was created to gather ideas on how to improve operational practices and identify investigative techniques within CSIS in order to enhance the level of sophistication of the Service's operations.

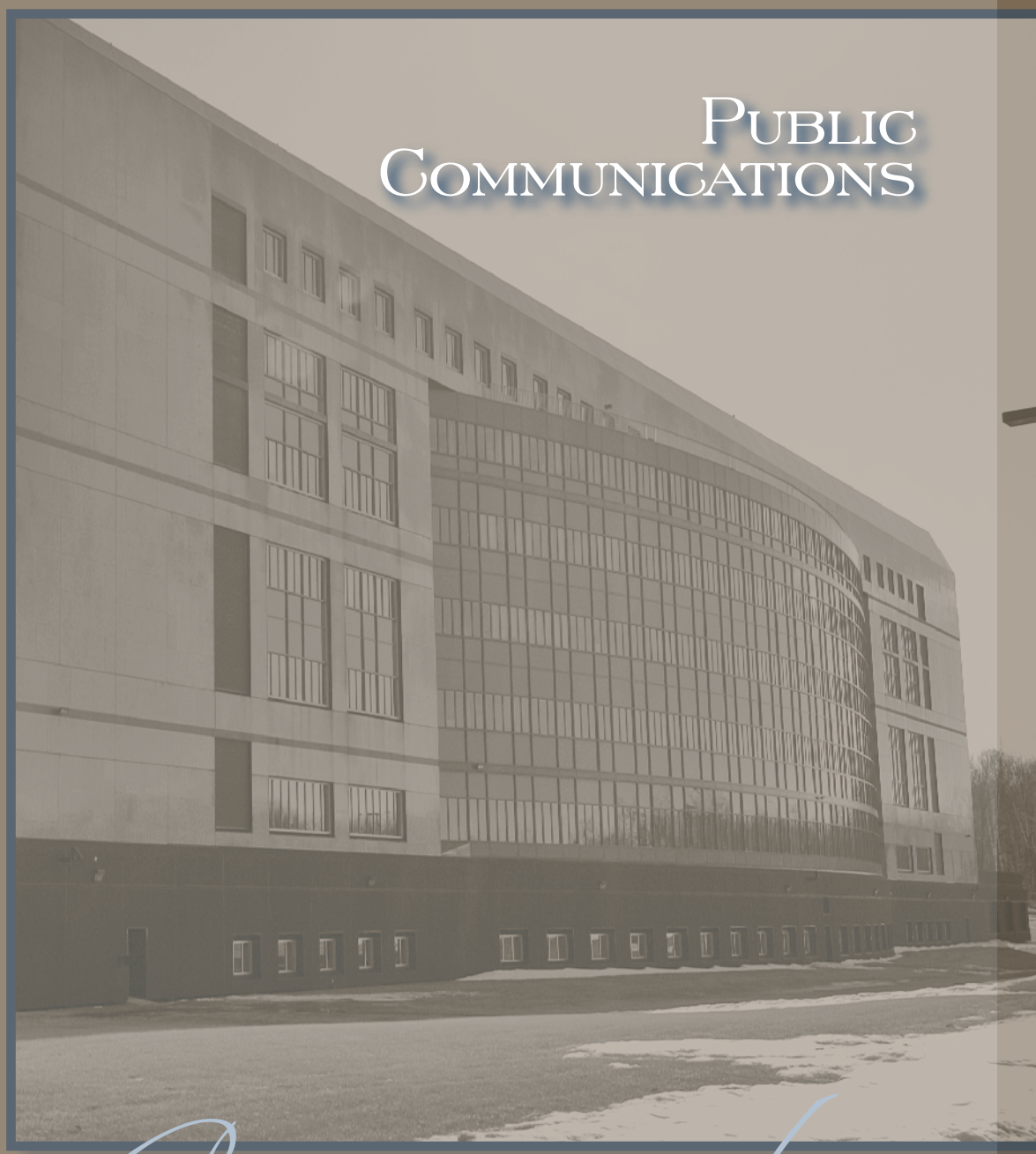
In the context of this working group, Service employees, federal partners, police forces, private companies and allied intelligence services were consulted and, as a result of this consultation, 22 recommendations were put forth, some of which will be implemented during the 2010-2011 fiscal period.

Corporate Planning

Established as a corporate priority in 2009-2010, a new integrated and multi-year corporate planning system and cycle were developed and introduced in the Service during this period. The work under-

taken culminated in the development of an overall 'CSIS Corporate Business Plan', based on the individual CSIS 'Branch Business Plans', and covering the 2010 to 2013 period.

It is anticipated that this new process will contribute to advancing the integration of planning and accountability within CSIS, a process which used to be carried out in a decentralized fashion prior to this new initiative. This plan will better articulate and align corporate priorities, directorate business plans, and financial and human resource allocations.



Public Communications

Communications

In 2009-2010, CSIS's public profile remained high, with more than 2,600 media reports referring to the Service during this period. The majority of references to CSIS in the media were in news items pertaining to legal cases such as those linked to security certificates and the 'Toronto 18' cases.

In most instances, CSIS cannot publicly confirm allegations reported in the media. However, where and when it can, CSIS does reach out to the public to keep Canadians informed, within unclassified parameters, so as to explain the Service's role, mandate and organization. For example, in 2009-2010, CSIS:

- responded to over 230 media queries;
- responded to more than 1,230 public queries (telephone and written);
- provided testimony by the Director or other high-level CSIS managers before various Parliamentary and Senate Committees;
- continued to distribute information through its Public Report, backgrounders and brochures;
- continued to provide updated information relating to CSIS on its public website.

Aside from its public and media communications program, the Service also participates in many outreach initiatives so as to better explain to various communities who we are and what we do. In 2009-2010, CSIS continued its efforts in this regard by providing briefings and presentations to academic and ethno-cultural communities, Canadian business leaders, non-government organizations, as well as universities and high-schools.

In 2009-2010, CSIS participated in regional events of the Federal Cross-Cultural Roundtable on Security (CCRS), in career fairs, employee recruiting events at universities and community festivals. The CSIS Director also delivered keynote speeches at the Canadian Association for Security and Intelligence Studies (CASIS) Conference in Ottawa and to the Royal Canadian Military Institute in Toronto. The Director was also interviewed by the McGill News alumni magazine.

Lastly, the CSIS website (www.csis-scrs.gc.ca) continued to be a popular Internet destination for those looking for information about the Service and on various issues associated with its work. In 2009-2010, more than six million hits were registered on the official CSIS website.

CSIS on the Internet

The CSIS website continues to be a popular Internet destination for those seeking official information about the Service. The following chart provides approximate figures about the number of times various pages on the CSIS site were viewed in 2009-2010:

*CSIS website 2009-2010**

Item(s) viewed	Number of views
Website (total views of all pages)	6,343,887
Backgrounders	58,696
Integrated Threat Assessment Centre (ITAC)	136,865
'Commentary'	219,036
'Perspectives'	35,974
Public Report (all years)	44,458
Recruitment information and job postings	3,383,071

** Numbers are approximate and do not include views of graphics on the site.*

Academic Outreach

CSIS launched its 'Academic Outreach Program' in September 2008. The purpose of the program is to promote a dialogue with experts from a variety of disciplines working in academic institutions and think tanks, in Canada and abroad. This allows CSIS to gain access to leading expertise—even if at times such expertise may conflict with the Service's own views—in order to refine our understanding of current and emerging security issues.

While the program allows the Service to better support and focus its intelligence collection efforts, it also allows CSIS to improve its analytical capacity and the quality of the assessments it prepares for government decision—and policy-makers. A more interactive relationship with the academic community also provides a platform from which to share insights on issues and developments relating to the Service's mandate, and to provide a better understanding within the community of the government's intelligence priorities.

Since the program's creation, there has been a significant interest on the part of experts to participate in activities sponsored by CSIS. These events have included four international conferences, numerous seminars and roundtable discussions, and a variety of 'CSIS Lunchtime Theatre Presentations' at the Service's National Headquarters covering issues that have either a direct or indirect impact on Canada's security environment.

During the course of 2009-2010, the discussions have covered a range of very focussed and broader, more strategic issues, including: China's rise, its place in the world and its potential impact on the global system; Iran's growing presence in Latin America; the global security and political impact of the recent economic downturn; terrorist financing; the possibility of nuclear terrorism; and the security dimension of climate change.

The Service's Academic Outreach Branch hopes that such valuable exchanges with experts from Canada and abroad will assist the Service in asking the right questions—and avoiding surprises—on issues of interest pertaining to both the Canadian and international security environments. Such exchanges will also allow CSIS to take a more holistic approach when reviewing and assessing national and international issues of interest. The 'Academic Outreach Program' has also solidified partnerships with other government departments. For example, Canada's International Development Research Centre (IDRC), Canada's Export Development Corporation (EDC) and Public Safety Canada were co-sponsors, along with CSIS, of one international conference and a series of seminars on issues of mutual interest to several government stakeholders which drew representatives of all departments and agencies from the intelligence community. Likewise,

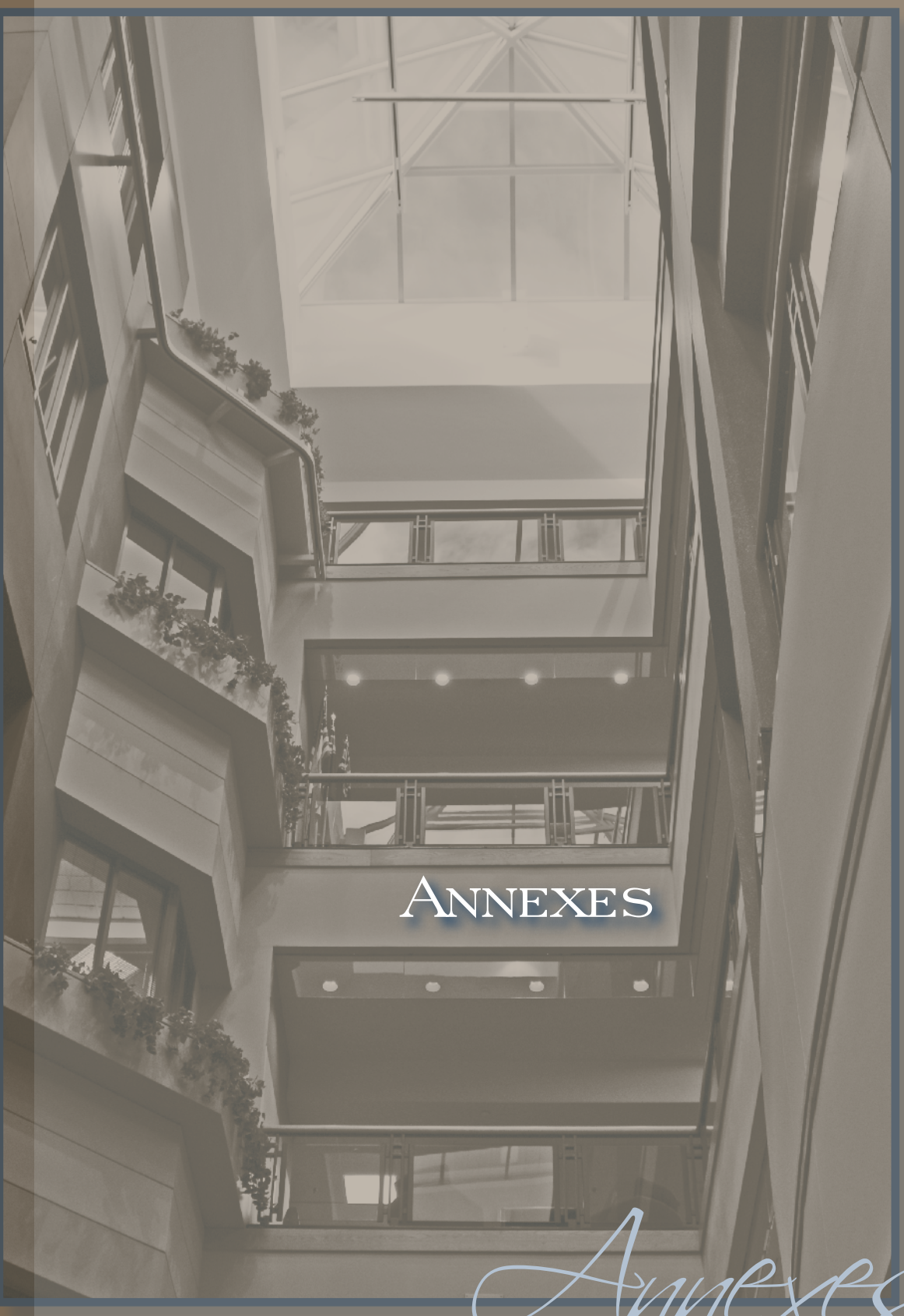
Academic Outreach presentations at the CSIS 'Lunchtime Theatre Series' presentations are open to members of the intelligence community.

Through this program, CSIS has also increased its support and participation in international outreach efforts such as the 'Global Futures Forum', which touch upon transnational threats and emerging issues of broad concern. The results of some of the Service's Academic Outreach activities are released on the CSIS website as part of the World Watch: Expert Notes series. This allows CSIS to share some of the findings and stimulate debate on intelligence and security issues of interest to all Canadians.

Community Involvement

While CSIS is primarily known for its intelligence work, it is also a workplace with a strong internal culture, sense of pride and community involvement, both at the Headquarters and Regional levels. In 2009-2010, CSIS employees continued to support various charitable causes. Donations by CSIS employees to the Government of Canada's Workplace Charitable Campaign (GCWCC) were once again record-setting for the Service. With a set goal of $225,000, CSIS employees contributed over $277,000, surpassing that goal by more than $52,000.

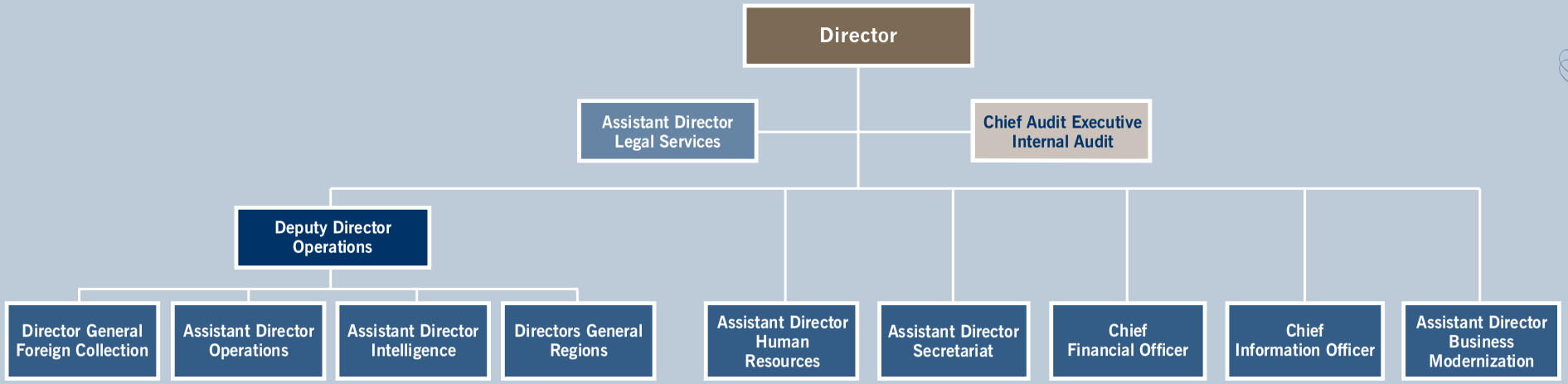
Additionally, employees organized several activities to raise a total of more than $12,000 for the Haiti Disaster Relief Fund. Furthermore, various other fundraising events were organized throughout the 2009-2010 period to raise money for a wide variety of other charities. Events such as 'Casual Fridays', where employees donate money to various charitable causes and, in turn, wear casual clothing to work on that specific day, raised thousands of dollars for a broad range of charities, in addition to the monies raised for the GCWCC and Haiti relief efforts.



Annexes

Annexes

Annex 1, Executive Organizational Chart



A new organizational structure was approved in September 2010 which will be reflected in the 2010-11 public report.

Annex 2, Contact us

National Headquarters:

Canadian Security Intelligence Service
P.O. Box 9732, Station T
Ottawa ON K1G 4G4

Tel. 613-993-9620 or 1-800-267-7685 toll-free (Ontario only)
TTY 613-991-9228 (for hearing-impaired, available 24 hours a day)

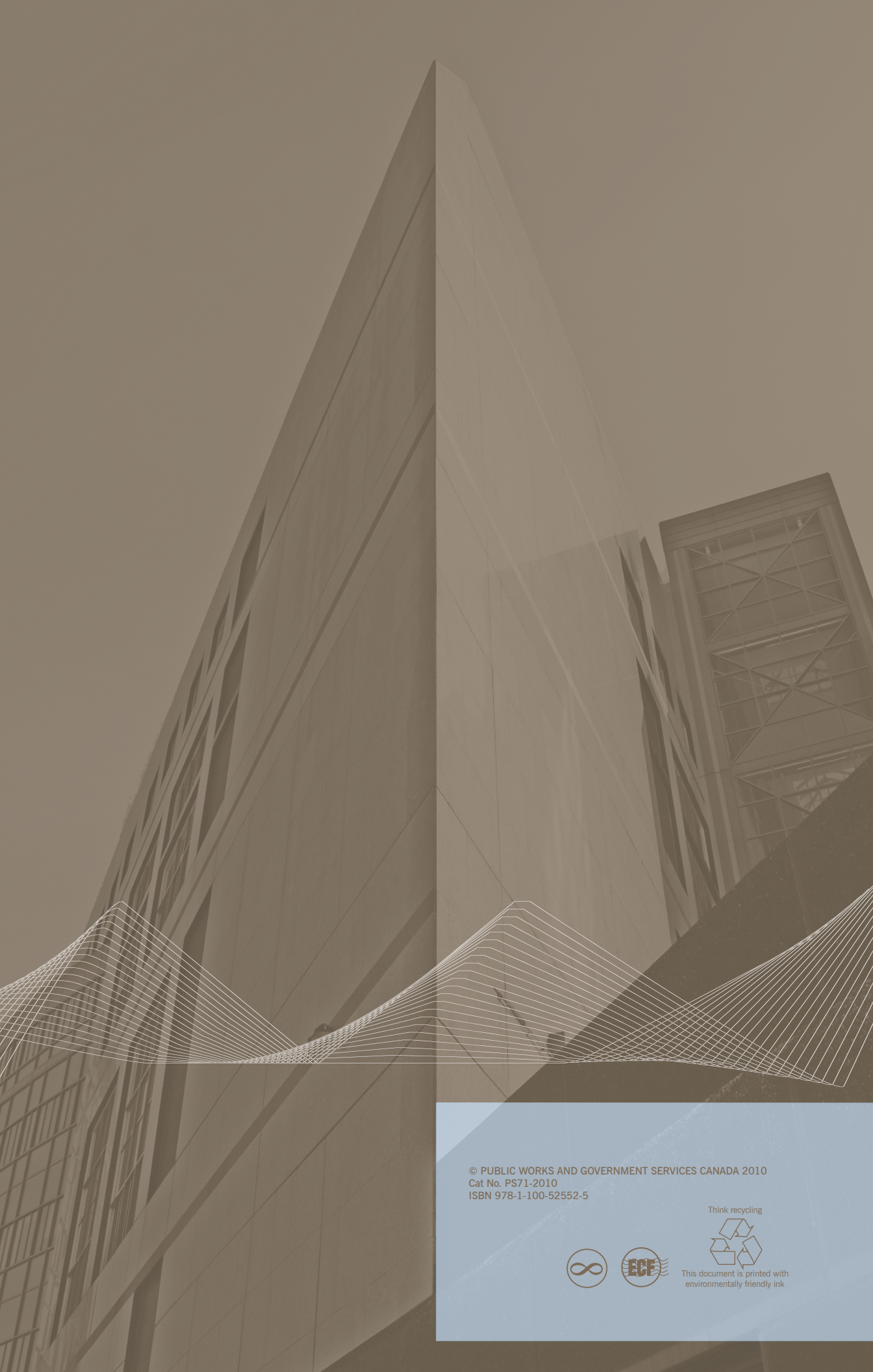
Media and Public Liaison Queries:

CSIS Communications Branch
P.O. Box 9732, Station T
Ottawa ON K1G 4G4
Tel. 613-231-0100

Regional Offices:

Atlantic Region	P.O. Box 126, Station Central Halifax NS B3J 3K5 Tel. 902-420-5900
New Brunswick District	P.O. Box 6010, Station A Fredericton NB E3B 5G4 Tel. 506-452-3786
Newfoundland and Labrador District	P.O. Box 2585, Station C St. John's NL A1C 6J6 Tel. 709-724-8650
Quebec Region	P.O. Box 2000, Station A Montreal QC H3C 3A6 Tel. 514-393-5600 or 1-877-223-2265 toll-free (Quebec only)

Quebec City District	P.O. Box 10043, Station Sainte-Foy Quebec QC G1V 4C6 Tel. 418-529-8926
Ottawa Region	P.O. Box 9732, Station T Ottawa ON K1G 4G4 Tel. 613-998-1679 or 1-800-267-7685 toll-free (Ontario only)
Toronto Region	P.O. Box 760, Station A Toronto ON M5W 1G3 Tel. 416-865-1480
Prairie (Alberta, Saskatchewan, Manitoba, Northwestern Ontario, Yukon, Northwest Territories, Nunavut)	P.O. Box 47009 62 City Centre Edmonton AB T5J 4N1 Tel. 780-401-7800 or 1-800-661-5780 toll-free (Prairie only)
Calgary District	P.O. Box 2671, Station M Calgary AB T2P 3C1 Tel. 403-292-5255
Saskatchewan District	P.O. Box 5089, Station Main Regina SK S4P 4B2 Tel. 306-780-5512
Manitoba District	P.O. Box 771, Station Main Winnipeg MB R3C 4G3 Tel. 204-954-8120
British Columbia Region	P.O. Box 80629, Station South Burnaby BC V5H 3Y1 Tel. 604-528-7400



Cat No. PS71-2010
ISBN 978-1-100-52552-5

Think recycling

This document is printed with environmentally friendly ink