Canadian Security Intelligence Service

Service canadien du renseignement de sécurité

/// 2018

CSIS PUBLIC REPORT

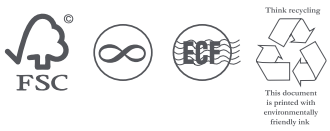
Canada

Aussi disponible en français sous le titre : *Rapport public du SCRS 2018*

www.canada.ca

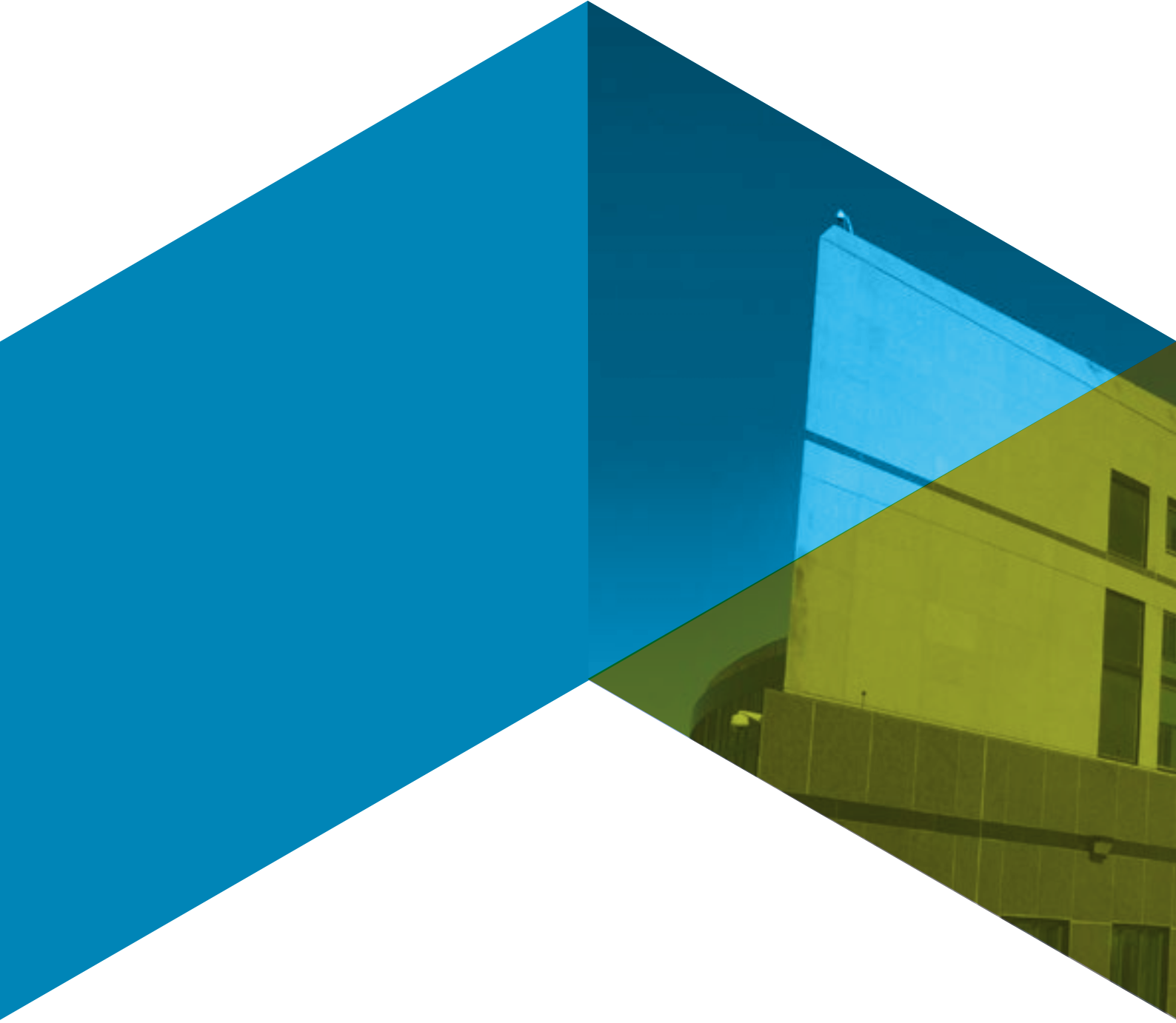
Published in June 2019

Cat No. PS71-2018
ISSN: 1188-4415



/// 2018 CSIS PUBLIC REPORT

/// TABLE OF CONTENTS



/// OUR VISION

"A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE".

/// MESSAGE FROM THE DIRECTOR

Almost 35 years ago, on July 16, 1984, the Canadian Security Intelligence Service (CSIS) came into existence.

As a new civilian security intelligence agency, CSIS entered a world that held significant challenges—some quite different than those we face today, and some that are very similar.

The international landscape of 1984 was still dominated by the Cold War, as the United States, the Soviet Union, and their respective allies, sought to protect and project their interests. At the same time, we saw the early days of a movement in Afghanistan that would evolve into Al Qaeda, a terrorist group that went on to carry out the 9/11 attacks. When the *CSIS Act* was written, a wiretap to intercept the communications of a threat actor could be done with alligator clips on a telephone wire and the internet, smartphones and artificial intelligence were more science fiction than reality. Similarly, information was locally available, stored in one place, and transmission was simple. Today, a single email may transit through multiple jurisdictions at the same time and be stored in a server on another continent across the ocean.

Terrorism remains the number one national security threat to public safety for Canada. Al Qaeda may not be as strong as it was two decades ago, but it still wields influence on likeminded groups around the globe. The threat posed by Daesh remains, even as its stronghold decreases. These groups and others inspire and radicalize individuals, including Canadians, to commit violence or travel to participate in terrorist activities overseas. The threat posed by those who then return to Canada, or were unable to leave in the first place, continues to be a priority for CSIS. Canada has also experienced first-hand the threat posed by individuals and online communities who harbour extreme right-wing views and are promoting or engaging in acts of violence. We have not only witnessed these inspired attacks: we have felt their impact. Using low-sophistication

tactics, such as vehicle ramming and firearms, attackers attempt to cause harm to achieve their goals. We are increasingly preoccupied by the violent threat posed by those looking to advocate/support/engage in racially motivated, ethno-nationalist, anti-government and misogynist violence.

While terrorism has occupied a significant portion of our collective attention for almost two decades, other national security threats—such as foreign interference and espionage—continued to persist and pose long-term, strategic challenges for Canada. Activities by hostile states are detrimental to Canada's economic, industrial, military and technological advantage, and have a corrosive effect on our democratic systems and institutions. Interference by foreign spies, or people acting on their behalf, remains the greatest danger. These hostile actors engage in sophisticated methods, leveraging technology and person-to-person methods. The scale, speed, range, and impact of foreign interference has grown as a result of the Internet, social media platforms, and the availability of cheaper and more accessible cyber tools. The use of cyber by hostile actors, a tool that did not exist when CSIS was created, poses enormous risk as Canadians increasingly live their lives and store their personal, and corporate, information online.

The threat environment today is complex, continuously evolving, diverse, and global. In today's globalized environment, we must reflect on the tools we have to monitor threats to Canadians that originate abroad as well, protecting Canada's national interests by understanding activities of hostile states.

Since its creation, CSIS has always strived to ensure its intelligence is relevant and faces challenges when its intelligence is used to protect national security through criminal investigations, prosecutions, enforcement actions by partners at CBSA and Public Safety, and national security reviews of foreign investments, to name

just a few. Providing this advice while protecting our sources—who put much at risk, and our methods and relationships—remains a challenge. So too does the massive volume and variety of digital communications, ubiquitous encryption, and other technological advancements challenge the Service's ability to collect intelligence. While tools such as encryption are essential for safeguarding Canadians and Canadian institutions, threat actors also exploit these developments to their advantage. At the same time, technological changes have prompted new online behaviours which have radically shifted how we understand privacy.

To pursue its mandate effectively, CSIS must be confident that it has the authorities and tools to fulfill its mandate to investigate and advise Government. A statute drafted in 1984 is not as relevant decades later, as both the Security Intelligence Review Committee and the Federal Court have highlighted. Modernizing the *CSIS Act* began with Bill C-44; had new authorities introduced in Bill C-51; and continues with the major changes proposed in Bill C-59 (An Act respecting national security matters). While this has addressed specific challenges and provides some modern authorities, there is still work to be done.

CSIS, as an organization, must remain vigilant in assessing whether our current authorities, tools and resources are keeping pace with the continuous changes in the threat, technological and legal landscape. Going forward, ensuring that CSIS employees have an updated legal framework and tools in place to carry out their mission continues to be an essential priority. This in turn ensures CSIS can provide timely and relevant intelligence to Government, enhancing our national security and interests in a complex global environment.

As the Director of CSIS, I take the greatest pride in the exceptional quality of our workforce. The people of CSIS serve their country extremely well, and they take their responsibility to protect Canada very much to heart, carrying out their duties in the knowledge that they are making us a safer country. As they are the organization's most valuable resource, ensuring that they have a safe, healthy and respectful workplace is essential.

In my role as Director, I am guided by the overarching objective of supporting excellence in fulfilling our core mandate of investigating and advising Government of threats to the security of Canada. I am proud to say that, in CSIS' most recent public opinion research, 95 per cent of respondents indicated that they place a great deal of importance on CSIS' role and a further 80 per cent indicated they trust that CSIS will safeguard their rights and freedoms.

At CSIS, accountability is at the centre of everything we do, and our compliance with the laws of Canada is paramount. It is only with the trust and confidence of Canadians that we have the social license to perform our duties. It is therefore incumbent upon the organization to demonstrate that we have earned that trust.

With that in mind, we are taking steps to be more transparent about our work. By engaging Canadians about the threats we're facing, we can better explain how our authorities allow us to fulfill our mission. We will continue to work with our partners in building protections against these threats.

As we approach our 35th anniversary, I reflect regularly on where we have been, and where we are going as an organization. What has not changed is that CSIS is committed to fulfilling our most important mission: to keep Canadians safe. And we will continue to do so in a manner that reflects this great country's values, and the trust that Canadians have placed in us.

David Vigneault, Director

/// THE RELEVANCE OF OUR WORK

CORE MANDATE

- Investigate activities suspected of constituting threats to the security of Canada
- Advise the Government of these threats
- Take measures to reduce threats to the security of Canada

THREATS TO THE SECURITY OF CANADA

- Terrorism
- Espionage and sabotage
- Foreign influenced activities detrimental to the interests of Canada
- Subversion of government through violence

PARTNERSHIPS

NEARLY 80 ARRANGEMENTS WITH DOMESTIC PARTNERS

OVER 300 ARRANGEMENTS WITH FOREIGN PARTNERS IN SOME 150 COUNTRIES

- Robust information sharing framework ensures conformity to Ministerial Direction

ACCOUNTABILITY

- Canadian public
- Minister of Public Safety
- Federal Court
- Security Intelligence Review Committee
- National Security and Intelligence Committee of Parliamentarians

DUTIES AND FUNCTIONS: *THE CSIS ACT*

SECTION 12

Investigate activities suspected of constituting threats to the security of Canada and to report on these to the Government of Canada

May take measures to reduce threats, if reasonable grounds to believe the activity constitutes a threat to the security of Canada

SECTION 13

Provide security assessments on individuals who require access to classified information or sensitive sites within the Government of Canada.

GOVERNMENT SECURITY SCREENING

✓ 76,550 Site Access
✓ 63,900 Government
✓ 220 Provinces
✓ 530 Foreign

SECTION 14

Provide security advice relevant to the exercise of the Citizenship Act or the Immigration and Refugee Protection Act

IMMIGRATION SCREENING

✓ 166,500 Citizenship
✓ 43,400 Perm Resident
✓ 58,400 Temp Resident
✓ 37,700 Refugees

SECTION 16

Conduct foreign intelligence collection within Canada at the request of the Ministers of Foreign Affairs and Defence

- Can only be carried out within Canada
- Must not target a Canadian citizen, permanent resident or corporation

Statistics as of end of fiscal year 2017-18.

DEPARTMENTAL RESULTS FRAMEWORK

CORE RESPONSIBILITY: SECURITY AND INTELLIGENCE

DEPARTMENTAL RESULTS

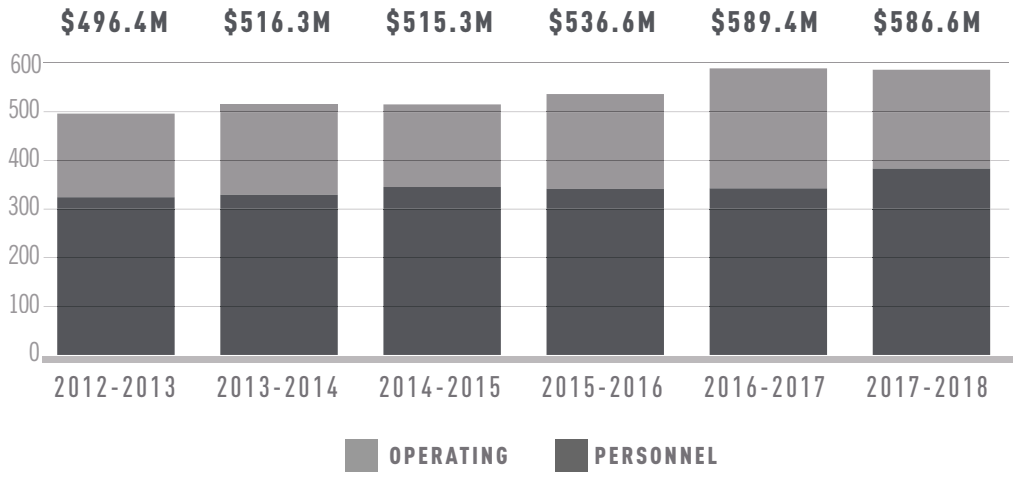
- CSIS obtains relevant information and intelligence to carry out its national security activities.
- CSIS intelligence informs government decisions and actions relating to Canada's security and national interests.
- CSIS threat reduction measures diminish threats to the security and safety of Canada and Canadians.
- The assessments of the Integrated Terrorism Assessment Centre inform Government of Canada decisions and actions relating to the terrorism threat.

PROGRAM INVENTORY

- Operational Program Management
- Regional Collection
- Operations Enablement
- Intelligence Assessment and Dissemination
- Security Screening
- Integrated Terrorism Assessment Centre

ACTUAL EXPENDITURES

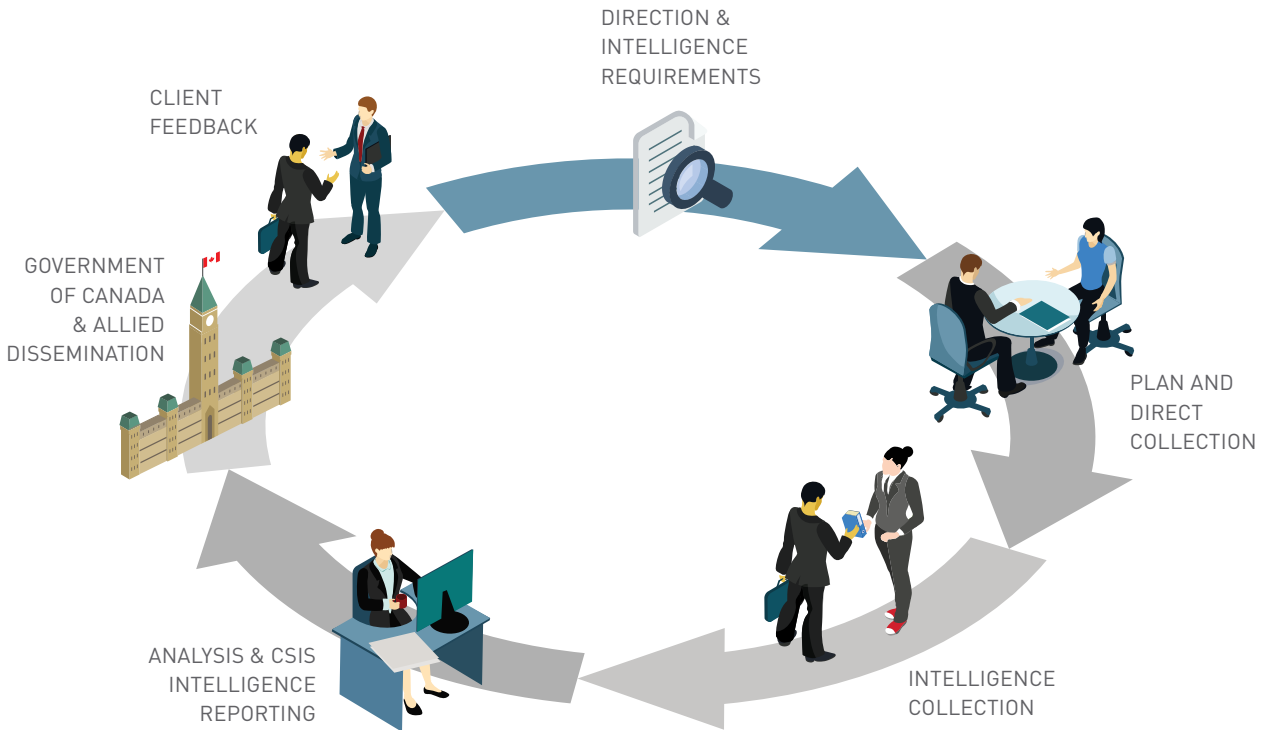
(MILLIONS OF DOLLARS)



THE INTELLIGENCE CYCLE

In order to fulfill its mandate, CSIS gathers intelligence information and disseminates it to appropriate government clients using a five-phase process, known as the "intelligence cycle".

1. Requirements and Direction
2. Planning
3. Collection
4. Analysis
5. Dissemination



1. Requirements and Direction

The *CSIS Act* gives CSIS the mandate to investigate activities suspected of constituting threats to the security of Canada, including espionage, sabotage, terrorism, foreign influenced activities detrimental to the interests of Canada and subversion of government through violence.

In keeping with this mandate, CSIS receives direction from the Government of Canada on the intelligence requirements of most importance, through multiple sources:

- Government Intelligence Priorities as established by Cabinet through discussion and consultation with the relevant Ministers and the Security and Intelligence community.
- Minister's Direction on Intelligence Priorities, which translates the Government Intelligence Priorities into specific collection direction for CSIS
- Regular meetings with domestic partners, such as Communications Security Establishment and the Royal Canadian Mounted Police, as well as with clients within the Government of Canada who are intelligence consumers.

2. Planning

The Government and Ministerial Direction on Intelligence Priorities, the CSIS Act and the needs of domestic partners and clients are all taken into consideration when developing the annual collection strategy.

Responding to this direction, CSIS establishes internal direction and annual collection plans to meet the intelligence needs of Canadian government departments and agencies.

3. Collection

CSIS uses a variety of methods to collect information on individuals and groups whose activities are suspected of constituting a threat to national security.

The information necessary to conduct an investigation is collected from various sources, including:

- Open sources such as newspapers, periodicals, academic journals, foreign and domestic broadcasts, official documents, and other published material; and
- Members of the public, human sources, foreign governments, Canadian partners, as well as through technical interception of communications and inquiry. Any intrusive measure, or those affecting the privacy of Canadians, requires obtaining a warrant, approved by the Minister, and authorized by the Federal Court.

4. Analysis

CSIS analysts use their knowledge of regional, national and global trends to assess the quality of all types of information gathered, analyze it and produce useful intelligence for clients and consumers.

CSIS analysts examine the information provided by other Canadian government departments and agencies, foreign intelligence agencies, intelligence collected through investigations, as well as open sources. The analysis process results in intelligence reports and threat assessments.

5. Dissemination and Feedback

CSIS disseminates intelligence products and assessments primarily to the Government of Canada and supporting law enforcement authorities. CSIS also disseminates intelligence to Five Eyes partners – a global intelligence alliance comprised of Canada, USA, UK, Australia and New Zealand – as well as other foreign

allied partners. An integral part of the intelligence cycle is collecting feedback on intelligence products from our partners. CSIS gathers product specific feedback from all partners, and routinely gathers requirements from the Government of Canada partners to help shape and drive collection and production efforts.

THREATS TO CANADA'S NATIONAL SECURITY

Terrorism in Canada: Inspired Violence

The terrorism threat landscape in Canada continues to evolve and is directly impacted by both domestic and international trends and events. There remains a persistent intent demonstrated by domestic actors to carry out a violent act of terrorism. Terrorism perpetrated by extremists who are inspired by terrorist groups such as Daesh and Al Qaeda, including those who seek to travel to join terrorist groups abroad, or those who radicalize, is the number one national security threat to public safety in this country. Investigating these threats remains a top priority for CSIS.

CSIS also remains concerned about the threat posed by those who harbor and support other forms of extremism. The globalization of terrorism, fueled by elaborate online propaganda by extremist groups, has expanded the breadth of radicalization and mobilization to violence. In some instances, individuals influenced by extremist ideology have travelled (or attempted to travel) abroad to participate in terrorist activity. Others have supported their extremist ideology through training, fundraising, recruitment and attack planning within Canada.

Recent terrorism activities in the West have been typically characterized by low-resource, high-impact acts, and usually inspired by terrorist groups such as Al Qaeda or extremists responding to Daesh's call for a 'virtual caliphate'. The increased use of low-sophistication and low-resource means is evident in the repeated use of vehicles and knives in attacks in Europe and North America. Despite the decrease in sophistication, the impact and lethality remains high as the perpetrators often strike soft targets. Daesh and AQ propaganda has provided guidance to their supporters on the use of small arms, vehicles and bladed weapons, offering suggestions on

how to inflict the most harm. Encouragement to use simple weapons can empower those who would otherwise be incapable of conducting a more complex terrorist attack.

An important part of terrorist messaging and recruitment is the use of media and social media. There has been a surge in Daesh media production as the group continues to spread its message by disseminating material by new means and alternative platforms (e.g. using platforms that do not require identification, reverting to the use of forums or using Darknet libraries to share links). The use of cyberspace by terrorist entities to enhance the security of their activities will remain a challenge for the security and intelligence community. Most notably, the increasing prevalence of encryption technologies allows terrorists to conceal the content of their communications and operate with anonymity while online. This allows them to evade detection by police and intelligence officials, presenting a significant challenge to governments' ability to investigate and prosecute threat actors.

Daesh has lost significant amounts of physical territory due to the military actions of an international coalition which includes Canada. It has now shifted away from a focus on statehood to increased calls for retaliation, and CSIS assesses that Daesh will continue its efforts to inspire and/or encourage operations abroad. Attacks undertaken by individuals whose radicalization is facilitated by learned tactics and online and emerging technologies are the direct result of aggressive terrorist media campaigns which intend to inspire more violence. The phenomenon of radicalization, both offline and online, remains a significant concern to Canada and its allies.

Today's threat environment is global. We have an obligation to fully investigate threat activities in Canada directed outside our borders. Within Canada, threat-related activities primarily targeting India and committed by a small number of Canada-based extremists who support violent means to establish an independent state within India have continued, mostly at a low level, since their peak in the mid-1980s. Recently, however, there has been an increase in observed threat activity, wherein Canada is being used as a base to support this view as well as attacks targeting India. These activities constitute a threat to the security of Canada. Canada must contribute to the international community's efforts to prevent violent attacks from happening in any country.

Canadian Extremist Travellers

The Government of Canada has continued to monitor and respond to the threat of extremist travelers. These are individuals who have a nexus to Canada—meaning they hold citizenship, permanent residency or a valid visa—and who are suspected of having travelled abroad to engage in terrorism-related activity. The phenomenon of extremist travellers—including those abroad, those who return, and those who are prevented from travelling—poses a range of security concerns for Canada. While Canada's share of this problem is small, we are not immune.

Approximately 250 of these extremist travellers with a connection to Canada have journeyed overseas, about half into Syria, Iraq, and Turkey, and the rest into Afghanistan, Pakistan, and parts of north and east Africa, with approximately 190 still abroad. These individuals have travelled in order to support and facilitate extremist activities, and, in some cases, to directly participate in violence. Approximately 60 individuals with a nexus to Canada who were engaged in extremist activities abroad have returned to Canada. Of these 60, only a relatively small number of them returned from Turkey, Iraq or Syria.

The conflict in Syria and Iraq has been unprecedented in drawing extremists to fight overseas since it began in 2011, with departures reaching a peak in 2014. CSIS is aware of approximately 100 (out of the 190) individuals with a nexus to Canada who are suspected of engaging in terrorism–related activity within this region. Several factors, including foreign authorities preventing entry at their borders, enhanced legislation in Canada deterring individuals from leaving, as well as Daesh's loss of vast swaths of territory, have all contributed to the decline in the number of individuals travelling to join extremist groups in Syria and Iraq.

Canada has not experienced high numbers of returning extremist travellers from the Syria–Iraq conflict zone. Return to Canada from this region has proven difficult, given the risk of death or capture by myriad extremist and other armed groups and possible lack of valid travel documents and funds with which to travel. Finally, given their ideological commitment to their cause, many Canadian extremists are likely to remain in the conflict theatre in the short to medium term.

CSIS takes the threat posed by returning fighters very seriously. These people have not only shown the resolve to travel and join a terrorist group, they have often received training or gained operational experience while abroad.

CSIS and other Government of Canada departments and agencies are well organized as a community to manage the threat posed by returning fighters.

/// INDICATORS OF MOBILIZATION TO VIOLENCE (IMV) A CANADIAN GOVERNMENT APPROACH

Extremist radicalization and mobilization to engage in terrorist activities are complex processes. CSIS has long understood that all who radicalize do not engage in violent activity. Some do not have the opportunity, means or commitment to put their ideas into action. In light of the terrorist attacks in Ottawa and Saint-Jean-sur-Richelieu in 2014—followed by the surge in extremist travellers who left Canada for Syria and Iraq—CSIS updated and enhanced its use of structured analytics to better detail the patterns and evolution of threat activities observed amongst Al Qaeda/Daesh-inspired violence. This research provides an enhanced perspective on concrete activities which signal intent, capability and planning and preparation of individuals mobilizing to terrorism. In cooperation with the RCMP, perspectives and best practices resulting from this research were shared with frontline law enforcement and national security practitioners to aid in assessing whether an individual is radicalized and/or mobilizing to terrorism.

These findings were published by CSIS in the report *Mobilization to Violence (IMV)/ Terrorism Research: Key Findings.*

Right-Wing Extremism

Extremism can stem from a complex range of ideologies. CSIS works closely on the threat of violent right-wing extremism with domestic and international partners, including the law enforcement community.

Right-wing extremism is driven by hatred and fear and comprises a complex range of individuals, subcultures and online communities. These individuals and groups cultivate grievances on issues as varied as gender, race, religion, sexual orientation and immigration. Rather than openly promoting outright violence, some of those holding extreme right-wing views often attempt to create a culture of fear, hatred and mistrust by exploiting real or imagined concerns when addressing an online audience. In doing so, they attempt to legitimise their beliefs and move from the fringes of society to the mainstream.

Social media is transnational by nature and allows not only individuals from within the milieu to share their extreme right-wing views but also their modus operandi and details of attacks thus inspiring others to conduct their own. They may find inspiration from international terrorist attacks and adopt similar low-sophistication tactics (vehicle ramming, firearms, etc.).

Canada has experienced several violent attacks since 2014, perpetrated by individuals influenced in whole or in part by right-wing extremism. Examples include the shooting of three RCMP officers in Moncton in 2014, the shooting at the Islamic Cultural Centre of Quebec City in January 2017 and the April 2018 van attack in Toronto. The recent attacks in New Zealand highlight that our partners are also facing similar, growing threats. Since 2014, all Five Eye partners have experienced violent attacks or plots perpetrated by individuals influenced, in whole or in part, by their extreme right-wing views.

CSIS continues to engage government and law enforcement partners on the right-wing extremism landscape and emerging threats and continues to provide extensive analytical advice. CSIS has increased its posture to gain a better understanding of the landscape in Canada, gain insight into the key players and assess the nature of the current threat environment.

The International Terrorism Landscape and Implications for Canada

Despite the collapse of Daesh in Iraq and Syria, they continue to dominate the landscape in the Middle East, where Al Qaeda or Al Qaeda-aligned-groups and Hizballah also operate, and in Asia and Africa. In Yemen, both Al Qaeda in the Arabian Peninsula (AQAP) and Daesh have continued to take advantage of the civil conflict there, making effective use of vast lawless areas to expand their ranks and enhance their capabilities. In West Africa, Northern Mali remains the epicenter of terrorist activities, where violent extremist organizations aligned with Daesh and Al Qaeda have increased the frequency and the complexity of their attacks throughout the Sahel. For example Al Qaeda in the Islamic Maghreb (AQIM) and affiliated groups have aggressively targeted Western interests in a series of attacks against hotels and restaurants popular with Westerners in Mali, Burkina Faso, and Côte d'Ivoire, killing over 60 people, including at least eight Canadians in two attacks. Canadians in this region continue to face a high likelihood of being kidnapped or targeted in terrorist attacks. For example, a Canadian worker died in an attempted kidnapping at a mining site in Burkina Faso, which was later claimed by Daesh.

AQ's Malian affiliate, Jamaat Nusrat Al Islam Wal Muslimin (JNIM), perpetrated complex, coordinated attacks against the French embassy and the Chief of Defence Staff Headquarters in Ouagadougou. In East Africa, AQ-aligned Al Shabaab remains the dominant terrorist group in the horn of Africa and continues to pose a major threat to regional stability, conducting a terror attack in Mogadishu that killed over 500 people. However, Daesh-Core's global reach makes Daesh-Somali supporters a growing threat to Canada's national security, particularly as some Al Shabaab supporters and sympathizers shift their allegiance to Daesh.

Daesh has also established and strengthened links with regional groups in Southeast Asia. Through online activity, Daesh radicalized and inspired supporters across Asia to conduct attacks in Bangladesh, Indonesia and the Philippines. In the Philippines, Daesh conducted a siege of Marawi City which lasted six months. The cohesion and cooperation of Daesh militants in the Philippines was largely unanticipated. A Canadian extremist perpetrated a Daesh-style, directed terrorist attack at a bakery in Dhaka, Bangladesh.

Espionage and Foreign Influenced Activities

As part of its mandate, CSIS investigates and advises the Government of Canada on threats posed by espionage and foreign influenced activities. These threats continue unabated and, in some areas, are increasing. Canada's advanced and competitive economy as well as its close economic and strategic partnership with the United States makes it an ongoing target of hostile foreign state activities. Furthermore, Canada's status as a founding member of the North Atlantic Treaty Organization (NATO), as well as participation in a number of other multilateral and bilateral defence agreements, makes it an attractive espionage target.

Canadian interests can be damaged by espionage activities through the loss of sensitive and/or proprietary information or leading-edge technologies, and through the unauthorized disclosure of classified government information. A number of foreign states continue to covertly gather political, economic and military information in Canada.

Taking advantage of the increasingly interconnected nature of today's digital world, foreign state actors have capitalized on computer network exploitation, using cyber tools to compromise computer networks and steal sensitive information on an unimaginable scale. These cyber intrusions can result in the theft of a significant amount of sensitive information to the serious detriment of Canada's economic and strategic interests. They can also lead to the loss of the personal data of Canadians. Beyond the world of cyber-espionage, computer network exploitation has also become an important tool supporting interference activities.

Foreign governments also continue to use their state resources and their relationships with private entities in order to conduct foreign-interference activities in Canada. These activities are carried out in a clandestine or deceptive manner or involve a threat, and target communities or democratic processes in this country. Foreign powers have covertly monitored and intimidated diaspora groups in order to fulfil their strategic and economic objectives. In many cases, influence operations are meant to support foreign political agendas, a cause linked to a conflict abroad, or to deceptively influence Government of Canada policies, officials, or

democratic processes. These activities continue to constitute a significant threat to Canada's national security and strategic interests.

Protecting our Democratic Institutions

Democratic institutions and processes, including elections, of nations worldwide are vulnerable and have become targets for international actors. Foreign threat actors, most notably hostile states and state-sponsored actors, are targeting Canada's democratic institutions and processes. While Canada's electoral system is strong, threat actors have sought to target its politicians, political parties, elections, and its media outlets in order to manipulate the Canadian public and interfere with Canada's democracy. Certain states can seek to manipulate and misuse Canada's electoral system to further their own national interests, while others may seek to discredit key facets of Canada's democratic institutions to reduce public confidence in the democratic system.

The Government of Canada recently announced its plan to safeguard Canada's upcoming 2019 election. In order to determine the nature of these threats, CSIS conducts investigations against specific threat actors who are believed to be targeting Canada through clandestine or deceptive means, or via the involvement of a threat to a person. As part of its mandate, CSIS is responsible for advising the Government of Canada on threat related activities. As a member of the Security and Intelligence Threats to Election (SITE) Task Force, CSIS works closely with Canadian partners, including the Communications Security Establishment, Royal Canadian Mounted Police, and Global Affairs Canada, and our international allies and partners, to share information on election security.

Economic Security

There has been a noticeable increase in economic espionage in Canada. Hostile foreign intelligence services or people who are working with tacit or explicit support of foreign states gather political, economic, commercial, or military information through clandestine means here in Canada.

Foreign states have engaged in espionage activities targeting Canada in order to fulfil their economic and security development priorities. This type of espionage has had ramifications for Canada, including lost jobs, corporate and tax revenues, and a diminished competitive advantage. Canadian commercial interests abroad are also targets of espionage activities, and Canadian entities in some foreign jurisdictions are beholden to intrusive and extensive security requirements.

With its economic wealth, open business environment and advanced infrastructure, Canada offers 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 (SOEs) and private firms with close ties to their government and/or intelligence services have pursued corporate acquisition bids in Canada, raising national security concerns. Corporate acquisitions by these entities pose potential risks related to vulnerability of critical infrastructure, control over strategic sectors, espionage and foreign influence activities, and illegal transfer of technology and/or expertise. CSIS expects that national security concerns related to foreign investments in Canada will continue, owing to the increasingly prominent role of SOEs and state-linked private entities in the economic strategies of some foreign governments.

As difficult as it is to measure, this damage to our collective prosperity is very real and is the reason more and more governments are beginning to openly discuss the changing security landscape with their businesses, their universities, and the general public. The national security community and the business community have a shared interest in raising public awareness of the scope and nature of state-sponsored espionage against Canada, and of its potential effect on our economic growth and ability to innovate.

CSIS continues to investigate and identify the threats that espionage and foreign influenced activities pose to Canada's national interests, and works closely with domestic and international partners in order to address these threats.

Cyber Threats to National Security

Cyber-espionage, cyber-foreign-influenced activities, and cyber-terrorism pose significant threats to Canada's national security, its interests, as well as its economic stability.

Cyber threat actors conduct malicious activities in order to advance their political, ideological and economic interests. They seek to compromise both government and private sector computer systems by utilizing new forms of technology, taking advantage of existing security gaps, and a general lack of cyber security awareness on the part of users. Such activities are collectively referred to as "Computer Network Operations", or CNOs. State-sponsored entities and terrorists alike are using CNOs directed against Canadian interests, both domestically and abroad. Canada remains both a target for malicious cyber activities, and a platform from which hostile actors conduct CNOs against entities in other countries.

/// COMPUTER NETWORK OPERATIONS

CNOs can be classified as either espionage-related, when their aim is to covertly acquire information without their victim's knowledge, or as true "cyber-attacks", when they are intended to cause disruption of services and/or damage to property and their victim is aware of their effects, though not necessarily the identity of the perpetrator.

State-sponsored cyber threat-actors use CNOs for a wide variety of purposes with the main goal of breaching the confidentiality of information, impacting the integrity of data or information databases or impacting the availability of information. These could include: disrupting critical infrastructure and services; interfering in elections; and, conducting disinformation campaigns, as well as stealing intellectual property and trade secrets. In addition, non-state actors such as terrorist groups also conduct CNOs in order to further their

ideological objectives. Examples of such activity include website defacement and the release of personal identity information.

Canada's National Cyber Security Strategy views cyber security as an essential element of Canadian innovation and prosperity. CSIS, along with partners, particularly the Communications Security Establishment (CSE), plays an active role in shaping and sustaining our nation's cyber resilience through collaborative action in responding to evolving threats of malicious cyber activity. While CSE and CSIS have distinct and separate mandates, the two agencies share a common goal of keeping Canada, Canadians and Canadian interests safe and secure. In today's global threat environment, national security must be a collaborative effort. As part of their mandate, CSE's role is to protect computer networks and electronic information of greatest importance to Canada, helping to thwart state-sponsored or criminal cyber threat activity on our systems. In responding to cyber threats, CSIS carries out investigations into cyber threats to national security as outlined in the *CSIS Act*. By investigating malicious CNOs, CSIS can uncover clues that help profile cyber threat actors, understand their methods and techniques, identify their targets of interest, and advise the Government of Canada accordingly.

Security Screening

Through its Government Security Screening and Immigration and Citizenship Screening programs, CSIS serves as the first line of defence against terrorism, extremism, espionage and the proliferation of weapons of mass destruction.

The Government Security Screening (GSS) program conducts investigations and provides security assessments to address threats to national security. The assessments are a part of an overall assessment and assist Government departments and agencies when deciding to grant, deny or revoke security clearances. Decisions related to the granting, denying or revoking of a security clearance lies with the department or agency, not with CSIS.

GSS also conducts screening to protect sensitive sites from national security threats, including airports, marine and nuclear facilities. It assists the RCMP by vetting Canadians and foreign nationals who seek to participate in major events in Canada, such as G7 meetings and royal visits. It provides security assessments to provincial, foreign governments and international organizations when Canadians seek employment requiring access to sensitive information or sites in another country. All individuals subject to government security screening must provide consent prior to being screened.

The Immigration and Citizenship Screening (ICS) program conducts investigations and provides security advice to the Canada Border Services Agency (CBSA) and Immigration, Refugees, and Citizenship Canada (IRCC) regarding persons who might represent a threat to national security. Through this program, CSIS provides security advice on permanent residence and citizenship applicants; persons applying for temporary resident visas; and persons applying for refugee status in Canada. Decisions related to admissibility into Canada, the granting of visas or the acceptance of applications for refugee status, permanent residence and citizenship rest with IRCC.

STATISTICS

IMMIGRATION AND CITIZENSHIP SCREENING PROGRAMS

REQUESTS RECEIVED*	2016-2017	2017-2018
Permanent Resident Inside and Outside Canada	58,500	43,400
Refugees (Front-End Screening)**	20,100	37,700
Citizenship	93,000	166,500
Temporary Resident	52,000	58,400
TOTAL:	**223,600**	**306,000**

***FIGURES HAVE BEEN ROUNDED**

****INDIVIDUALS CLAIMING REFUGEE STATUS IN CANADA OR AT PORTS OF ENTRY**

GOVERNMENT SCREENING PROGRAMS

REQUESTS RECEIVED*	2016-2017	2017-2018
Federal Government Departments	58,400	63,900
SITE ACCESS		
Free and Secure Trade (FAST)	13,900	8,600
Transport Canada (Marine and Airport)	47,200	47,900
Parliamentary Precinct	1,900	2,600
Nuclear Facilities	14,500	10,300
Provinces	210	220
Others	4,200	3,800
Foreign Screening	520	530
Special Events Accreditation	3,300	2,600
TOTAL:	**144,130**	**140,450**

***FIGURES HAVE BEEN ROUNDED**

/// THE EXCELLENCE OF OUR PEOPLE

CANADIAN SECURITY INTELLIGENCE SERVICE

CSIS IS A TRUE NATIONAL SERVICE, AND, AS SUCH, ITS RESOURCES AND PERSONNEL ARE GEOGRAPHICALLY DISPERSED ACROSS CANADA. THE GEOGRAPHIC CONFIGURATION, ILLUSTRATED BELOW, ALLOWS CSIS TO CLOSELY LIAISE WITH ITS NUMEROUS FEDERAL, PROVINCIAL AND MUNICIPAL PARTNERS ON SECURITY ISSUES OF MUTUAL INTEREST.

CSIS ACROSS CANADA

The people of CSIS are a highly committed and professional group who work day in and day out to keep Canadians safe, while safeguarding their rights and freedoms.

Just like the people of Canada, we are a diverse workforce. Our diversity allows us to better understand the demographics of the Canadian communities we protect and gives us better tools to collect relevant and accurate intelligence.

With this in mind, CSIS continues to attract and retain a top performing and diverse workforce. Our team is passionate about promoting and maintaining a culture of operational excellence, employee engagement and inclusiveness where work is meaningful, employees are valued, and collaboration is celebrated.

CSIS has been recognized for innovation and leadership in the area of mental health and wellness. By building employee resilience and ensuring the well-being of our employees, CSIS is strategically situated to serve Canada and Canadians to the best of our abilities, while ensuring everyone is fully able to contribute to the fulfilment of our mission.

DEDICATED TO PROMOTING HEALTH AND WELLNESS

CSIS has adopted a holistic, team approach by taking into account the organizational efforts of prevention, promotion and intervention, while also considering the physical and psychological well-being of individual employees in the organization. Underpinning this approach are fundamental principles including diversity, communication, engagement, values and ethics, respect and civility, and leadership at all levels. At CSIS, everyone has a responsibility to ensure a healthy, safe and respectful work environment.

In an effort to promote culture change around mental health, CSIS developed and designed a Psychological Health and Safety Toolkit for Managers. This innovative and introspective tool was designed to provide managers and supervisors with questions to ask themselves around the thirteen psychosocial factors listed

in the National Standard for Psychological Health and Safety. Answering these questions gives direction to managers on how they can support and promote a psychologically healthy, safe and respectful workplace. Due to overwhelmingly positive feedback, a second toolkit was created in 2017 – A Toolkit for Employees.

BUILDING EMPLOYEE RESILIENCE

CSIS launched the Road to Mental Readiness (R2MR) Training for all employees in September 2017 as a preventative initiative to develop resilience in employees and destigmatize mental health issues in the workplace. This initiative helps reduce the potential of developing operational stress injuries, including post-traumatic stress, of personnel working in a high-stress environment. The Department of National Defence, which created and developed R2MR, provided "Training for Trainers" at CSIS. CSIS also hosted representatives from several other government departments in this training.

The Mental Health Commission of Canada published the Final Report for the Case Study to Implement the National Standard for Psychological Health and Safety. This concluded a three year research project in which CSIS, as one of 40 organizations across Canada, participated in the process of implementing The National Standard. The initial results of the Case Study Research Project showed that CSIS made substantial implementation progress across all five elements of the Psychological Health and Safety Management System. The final report provides a summary of promising practices and lessons learned in the journey to promote employee psychological health and safety.

In order to sustain these implementation efforts, CSIS signed on to participate in a Sustainability Project. The final results of the Sustainability project are available at www.mentalhealthcommission.ca.

RECRUITING

CSIS recruiting staff regularly attend events across Canada to find talent. They participate in information panels, promote CSIS careers at networking events, and, participate in university and college job fairs across the country.

CSIS has added a pilot to its proactive recruiting model by including on-site interviews. These give hiring managers valuable face-to-face time with potential applicants and, in turn, provide future hires with the opportunity to ask questions in person.

CSIS continues to foster recruiting partnerships with our federal partners through joint job fairs across Canada. Branded as the Federal Safety Security and Intelligence Career Fair (FSSI), the partners are committed to sharing best practices and recruiting talent to work in public safety. The partners include the Royal Canadian Mounted Police (RCMP), Public Safety (PS), Canada Border Services Agency (CBSA), Correctional Service Canada (CSC), Communications Security Establishment (CSE) and the Department of National Defence (DND).

GENDER-BASED ANALYSIS +

The Government of Canada expects that all policy proposals brought forward for consideration are informed and shaped by robust gender-based analysis. GBA+ is an analytical process used to assess how diverse groups of women, men and non-binary people may experience policies, programs and initiatives. The "plus" in GBA+ acknowledges that GBA goes beyond biological (sex) and socio-cultural (gender) differences. GBA+ also considers many other identity factors, like race, ethnicity, religion, age, and mental or physical disability.

To that end, CSIS has taken steps towards decision-making based on subject matter expertise, assessments and qualitative and quantitative analysis. This approach helps ensure that efforts are focused on threat activities and do not target Canadian communities based on bias or assumptions.

Consideration of GBA+ identity factors has been incorporated in our planning and program decisions in a number of areas. For example, CSIS currently delivers unconscious bias training to all new employees, supervisors and interviewers. A CSIS task force has been looking at areas where a formal GBA+ framework can be applied to ensure that CSIS effectively prioritizes its resources and investigative efforts.

GBA+ will specifically assist CSIS in:

- Prioritizing and focusing operational activities based on evidence-based decision-making.
- Supporting operational desks with enhanced resourcing / targeting / collection initiatives;
- Better understanding CSIS targeting activities, allowing for refined initiatives;
- Enforcing the compliance with policies and procedures in place to protect rights and freedoms.

CSIS will continue to make efforts to allow for more strategic and comprehensive integration of GBA + across the Service.

CSIS EMPLOYEES

3,200+ EMPLOYEES

WOMEN **48%**

MEN **52%**

16% MEMBER OF VISIBLE MINORITIES

2% ABORIGINAL PEOPLES

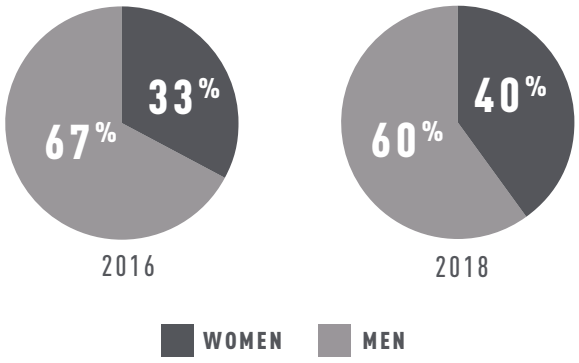
4% PERSONS WITH DISABILITIES

18% FOREIGN LANGUAGES

112 FOREIGN LANGUAGES KNOWN

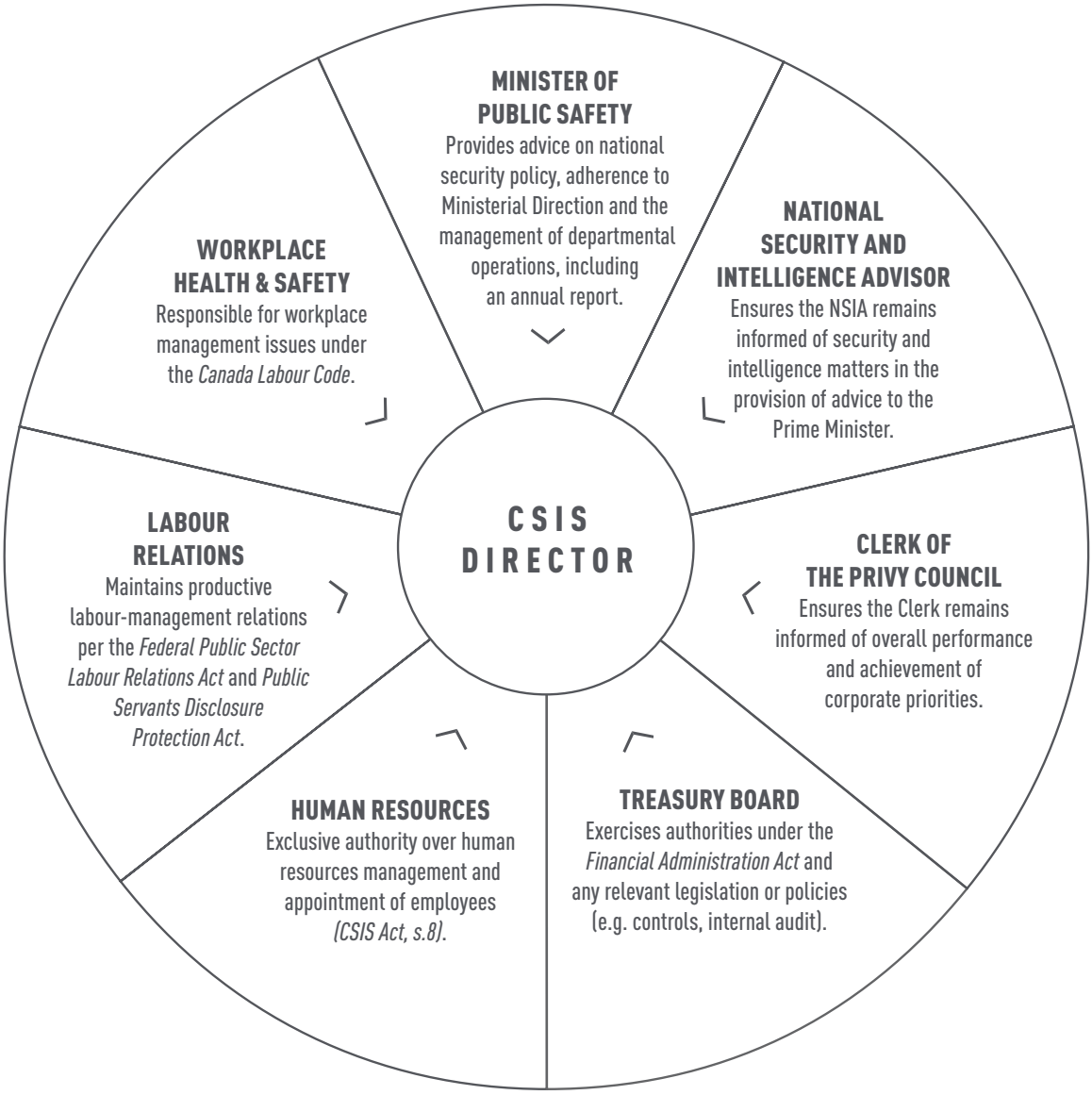
68% BILINGUAL

EXECUTIVE EMPLOYEES WHO SELF-IDENTIFY AS FEMALE



/// THE CONFIDENCE OF CANADIANS

ACCOUNTABILITIES OF THE CSIS DIRECTOR



LEGAL

Ensures that CSIS and its employees act lawfully in the conduct of its affairs and operations.

REVIEW

Ensures that CSIS responds to inquiries from the Security Intelligence Review Committee (SIRC) in the fulfillment of its statutory review function.

MANDATORY REPORTING

Ensures compliance with government reporting requirements, such as the Main Estimates, the Management Accountability Framework, Access to Information, and the Treasury Board Policy Suite.

PARLIAMENT

CORE MANDATE

· Public Accounts
· Government Operations and Estimates
· Standing Senate Committee on National Security & Defence
· Standing Committee on Public Safety & National Security

NATIONAL SECURITY & INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS (NSICOP)

Ensures that CSIS responds to inquiries in the fulfillment of its mandated review function.

OFFICERS & AGENTS OF PARLIAMENT

Ensures that CSIS responds to Agents and Officers of Parliament, including:

· Auditor General of Canada
· Information Commissioner
· Privacy Commissioner
· Parliamentary Budget Officer
· Commissioner of Official Languages

Ensures that CSIS responds to various government coordination bodies, including:

· Chief Statistician
· Chief Information Officer
· Ombudspersons
· Canadian Human Rights Commission

ACCOUNTABILITY AND RETAINING THE TRUST OF CANADIANS

As an intelligence agency it should surprise no one that much of what CSIS does is, and will remain, invisible to Canadians. Successful operations that identify and mitigate threats must be carried out clandestinely in order to be effective. Nevertheless, the way in which CSIS conducts that work is subject to considerable oversight and accountability.

Since CSIS' inception in 1984, the Security Intelligence Review Committee (SIRC) has been the independent review agency, reporting to Parliament on the operational activities of CSIS, and hearing public complaints. The Prime Minister of Canada is responsible for SIRC.

In addition, new legislation has led to the creation of the newly formed National Security and Intelligence Committee of Parliamentarians (NSICOP), which offers for the first time, a whole of government examination of the national security function.

Over the years, SIRC and CSIS have developed an open exchange of information to support SIRC investigations; CSIS is currently cultivating the same transparent relationship with NSICOP. CSIS works diligently to ensure SIRC and NSICOP have timely access to documentation required to satisfy their investigations.

CSIS has also established an operational compliance framework, ensuring that compliance is woven into the fabric of our organization's culture, in an effort to assure the Federal Court, the Government of Canada and Canadians that CSIS holds compliance with the laws of Canada as paramount.

CSIS welcomes any changes that contribute to an increase of public trust, while continuing its efforts to safeguard national security.

TRANSPARENCY

The confidence of Canadians in the national security efforts of CSIS is fundamental to our legitimacy, operational effectiveness, and institutional credibility. While certain information on our activities and interests must remain protected, CSIS is committed to making information about some of the activities more transparent to Canadians, ensuring there is no risk or compromise to national security. That is why CSIS is committed to providing clear and concise information about our role and mandate. Engaging Canadians on the legal framework under which we conduct national security activities, while balancing the privacy rights of Canadians, is a priority for CSIS. Through public forums, public communications, stakeholder engagement and social media platforms, CSIS endeavours to communicate transparently about our decision-making processes and national security activities. CSIS continues to look for opportunities to engage with Canadians in order to ensure their trust and confidence.

ATIP STATISTICS

	2016-2017	2017-2018
NUMBER OF *PRIVACY ACT* REQUESTS RECEIVED DURING THAT PERIOD	529	844
NUMBER OF *ACCESS TO INFORMATION ACT* REQUESTS RECEIVED DURING THAT PERIOD	491	851
NUMBER OF INFORMAL REQUESTS RECEIVED DURING THAT PERIOD	342	187

CSIS FOREIGN COOPERATION

The work of intelligence agencies today is transnational, and the increased 'globalization' of threats cannot be countered in isolation. Cooperation with foreign agencies provides CSIS access to timely information linked to a number of potential or specific threats, and allows the Service—and, in turn, the Government of Canada—to obtain information which might otherwise not be available.

In response to the evolving international threat environment over the past two decades, CSIS expanded its international presence to address increased domestic and international threats to Canadians and Canada's national interests.

CSIS has more than 310 foreign relationships in some 150 countries, each authorized by the Minister of Public Safety and Emergency Preparedness and supported by the Minister of Foreign Affairs, in accordance with s.17(1)(b) of the *CSIS Act*.

Since its inception in 1984, CSIS has reviewed and assessed its foreign relations based on a number of factors. CSIS reviews various yearly government assessments (e.g. Global Affairs Canada human rights reporting; US State Department Country Reports) and regular reporting from non-governmental entities (e.g. Amnesty International; Human Rights Watch; reporting from established media outlets etc.) on all countries with which CSIS has implemented a Ministerially-approved arrangement.

HUMAN RIGHTS CONSIDERATIONS

The human rights reputation of the agencies with which CSIS engages is not something which the Service takes lightly. CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency, and in all situations, it must and does comply with Canada's laws and legal obligations in sharing information with foreign entities.

The September 2017 Ministerial Direction (MD) on Avoiding Complicity in Mistreatment by Foreign Entities requires CSIS to monitor its foreign arrangements on a number of factors, including human rights and the risk of mistreatment, and impose restrictions on information sharing if it is assessed that a foreign entity is engaging in, or contributing to, mistreatment. In March 2018, CSIS implemented an additional mechanism of 'Restrictions' which add additional levels of review and approvals on proposals to exchange information in instances where such serious human rights concerns exist.

CSIS must also assess and attempt to mitigate potential risks of mistreatment prior to sharing certain types of information with foreign entities. Mitigation efforts include—but are not limited to—obtaining updated assurances from a foreign agency. Such assurances are sought to ensure the foreign agency understands and abides by CSIS expectations—and those of the broader GC—regarding the use of information provided by CSIS *vis-à-vis* human rights, including the treatment of detainees. Assurances outline to foreign agencies expectations that individuals will not be mistreated in any way as a result of information exchanges with the foreign agency, and will be treated in a manner consistent with domestic and international law, including the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

In accordance with the 2017 MD, the Service is also required to provide, on an annual basis, details to the Minister of Public Safety and Emergency Preparedness and to the National Security Intelligence Committee of Parliamentarians on 'substantial risk' cases where this direction was engaged, including the number of high-risk information sharing proposals reviewed by the CSIS Information Sharing Evaluation Committee (ISEC) — or those referred by ISEC to the CSIS Director—for decision. ISEC is a committee of senior officials from CSIS and Global Affairs Canada, advised by the Department of Justice. Such requests are sent to ISEC for review where there is a potential risk that sharing information on a specific case with a foreign entity may result in the mistreatment of an individual, and it is initially assessed at the Branch level that caveats, assurances and/or other factors may not mitigate the potential risk. ISEC then assesses whether or not there is a

substantial risk[1] as defined in the MD that the proposed information sharing with the foreign entity may result in the mistreatment of an individual.

During the 2017/18 reporting period, ISEC considered a total of four cases wherein 'substantial risk' as defined in the MD[1] was involved. Two of those requests were subsequently referred to the CSIS Director for decision, one of which was approved when it was determined there were sufficient mitigation measures in place to reduce the risk well below the 'substantial' threshold. The other case referred to the Director during that period was not approved, as it was assessed that the 'substantial risk' threshold could not be lowered enough through mitigation measures.

ACADEMIC OUTREACH

The Academic Outreach program at CSIS affords employee access to leading thinkers who can provide unique insights into a range of issues that have an immediate and long-term impact on Canada's security environment. It may happen that some of our academic partners hold ideas or promote findings that conflict with our own views and experience, but this is one of the reasons why we initiated the program. We believe there is value in having informed observers challenge our thinking and approaches.

The program helps CSIS focus its intelligence collection efforts and improve its analytical capacity. Reciprocally, a more interactive relationship with the academic community allows CSIS to share some of its own expertise and interests, which in turn can help scholars—political scientists, economists, historians, cyber security experts, psychologists, etc—to identify new avenues of research.

[1] *"Substantial risk" is defined in the Ministerial Direction on Avoiding Mistreatment by Foreign Entities as "a personal, present and foreseeable risk of mistreatment. In order to be 'substantial', the risk must be real and must be based on something more than mere theory or speculation. In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment; however, in some cases, particularly where the risk is of severe harm, the 'substantial risk' standard may be satisfied at a lower level of probability."*

The Academic Outreach program promotes partnerships with other government departments. Global Affairs Canada, the Privy Council Office, Immigration, Refugee and Citizenship Canada, the Department of National Defence, the Communications Security Establishment and the Canada Border Services Agency have all provided support to its workshops and programming. The AO program also serves as an important tool to strengthen partnerships with dozens of foreign partners and provides an opportunity for members of the intelligence community across government to exchange on timely and relevant security issues facing our country.

New legislation: C-59 – what does it mean for CSIS?

CSIS must understand, investigate and respond to a complex and evolving global threat environment.

Terrorists today are increasingly able to communicate securely because of the prevalence of strong encryption. Threats to Canada can also materialize from across the world. This poses enormous operational challenges.

Bill C-59 was tabled in the House of Commons in June 2017. It identifies lawful authority for longstanding collection activities and modern investigative techniques. It proposes a robust and transparent regime in law for dataset collection, retention and its use, as well as establishing in law an authorization regime for otherwise unlawful activities, modeled closely on safeguards in place for Canadian law enforcement. These changes will ensure that CSIS can respond to the evolving threat landscape and continue its vital role in the protection of Canada and Canadians. In order to keep pace with this evolving threat environment and the legal landscape, CSIS will continue to assess whether our current authorities, tools and resources enable us to carry out our mission.

CHANGES TO CSIS INVESTIGATORY POWERS, OVERSIGHT AND REVIEW UNDER

AN ACT RESPECTING NATIONAL SECURITY MATTERS, 2017 (BILL C-59)

The Canadian Security Intelligence Service (CSIS) is mandated to investigate threats to the security of Canada at home and abroad, to advise the government of Canada of these threats, and take measures to reduce such threats. An *Act Respecting National Security Matters* aims to clarify CSIS authorities, and introduce enhanced oversight and review institutions.

ACCOUNTABILITY

OVERSIGHT

INTELLIGENCE COMMISSIONER

- Independent oversight, plays a quasi-judicial role in reviewing specific Ministerial decisions.
- Approves Minister's decisions regarding *classes* of otherwise unlawful activities; *classes* of Canadian datasets; *retention* of foreign datasets; and *exigent queries* of datasets.

NATIONAL SECURITY AND INTELLIGENCE REVIEW AGENCY (NSIRA)

- Mandate to review security and intelligence activities of any federal department/agency.
- Mechanism to report non-compliance to the Minister (who may report to Attorney General) and refer unlawful dataset use to the Federal Court.

OPERATIONS

JUSTIFICATION

Creates a limited **justification** to commit (or direct) acts or omissions that would otherwise be unlawful to fulfill its mandate.

KEY CHANGES

- Framework for otherwise illegal acts or omissions by designated employees and human sources.
- All acts or omissions reported to NSIRA.

DATASETS

Creates a clear new authority, with accountability and transparency, to collect, retain, and use **datasets** of *non-threat-related, personal* info to fulfill its mandate.

KEY CHANGES

- Allows collection/retention/use of such datasets for CSIS duties and functions (s. 12, 12.1, 15, 16).
- Includes data incidentally collected under warrant.

THREAT REDUCTION

Specifies when a **threat reduction measure** (TRM) warrant is required to comply with the Charter, and creates a list of measures permitted under warrant.

KEY CHANGES

- Prohibition against torture, detention, property damage causing injury.
- All authorized TRM reported to NSIRA.