Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

CSIS Public Report 2023

A safe, secure and prosperous Canada through trusted intelligence, advice and action.
Des renseignements, des conseils et des interventions fiables pour un Canada sûr et prospère.

Canada

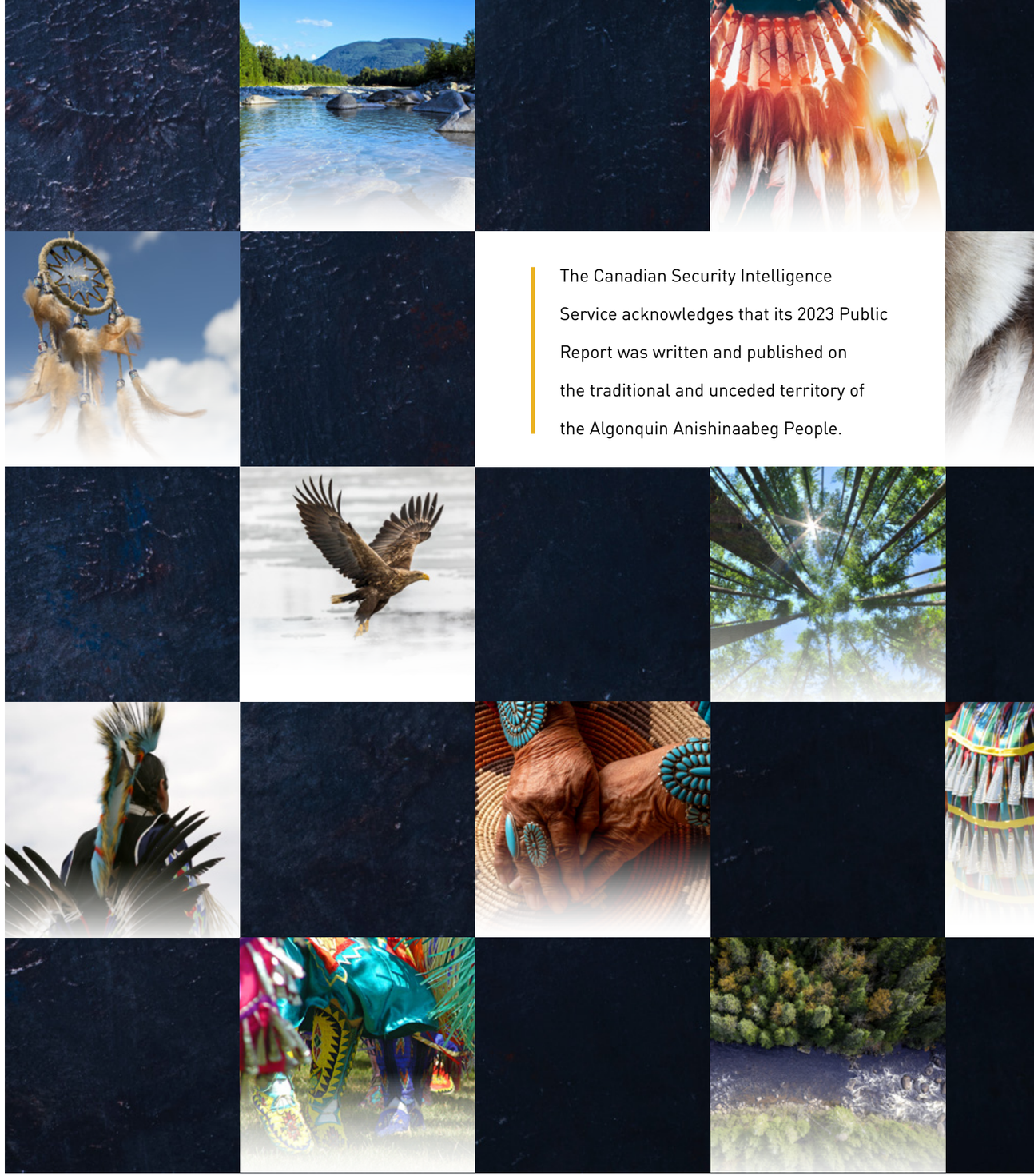
ISSN: 1495-0138

Catalogue Number: PS71E-PDF

Aussi disponible en français sous le titre : *Rapport public du SCRS 2023*

www.canada.ca/CSIS

Published in March 2024



The Canadian Security Intelligence Service acknowledges that its 2023 Public Report was written and published on the traditional and unceded territory of the Algonquin Anishinaabeg People.

Table of Contents

Message from the Director of the Canadian Security Intelligence Service

CSIS' National Headquarters is located in Ottawa, Ontario.

Director's Message

Year in Review: A Significant Period for National and International Security

Many Canadians considered Canada's security intelligence service like never before in 2023. CSIS and its work was the subject of more media stories than ever before. This robust media coverage on national security matters propelled our work into the spotlight, and as a result, helped shape the national conversation.

Events that transpired and topics that emerged last year, which are discussed in this report, such as foreign interference and espionage, will continue into 2024 and beyond. These extraordinary events have and will continue to set the stage for our country to reflect and have a mature conversation on national security. For example, the Business Council of Canada shares our concerns regarding the need to do more to protect Canadian businesses from research theft and the need to bolster our collective economic security with better information sharing practices. These discussions on the requirements and expectations of Canada's security intelligence service are timely and needed. However, they need to go beyond the results of public inquiries and program reviews. Our democracy and our social cohesion depend on it.

While I previously committed to stop saying "this was an unprecedented year for CSIS" in many ways, 2023 was a truly exceptional year in CSIS' nearly 40-year history.

The unauthorized disclosure of CSIS and Government of Canada intelligence products on multiple occasions dominated the media landscape and reverberated in Parliament, leading to the establishment of an independent special rapporteur on foreign interference and ultimately, a public inquiry on foreign interference. Canadians became aware of the extent to which foreign states interfere in Canada's affairs, and target and harass diaspora communities in Canada.

In June, a Canadian citizen and Sikh community leader, Hardeep Singh Nijjar, was murdered in British Columbia. In September, the Prime Minister, Justin Trudeau, made a statement in the House of Commons stating that Canadian security agencies had been actively pursuing credible allegations of a potential link between Government of India agents and the killing of Nijjar. The Prime Minister stated that the protection of Canadian citizens and the defence of Canadian sovereignty were fundamental. He stated

La Poile River, Newfoundland and Labrador.

that the Government's top priorities were for law enforcement and security agencies to ensure the continued safety of all Canadians, and for all steps to be taken to hold perpetrators of this murder to account.

In 2023, the world became less secure. Russia's illegal invasion of Ukraine waged on. The Kremlin continued to strike civilian areas and critical infrastructure with missiles and drones targeting Ukraine and Ukrainians. Russia continues its efforts to consolidate territory and legitimize a land and resource grab, redrawing borders by force.

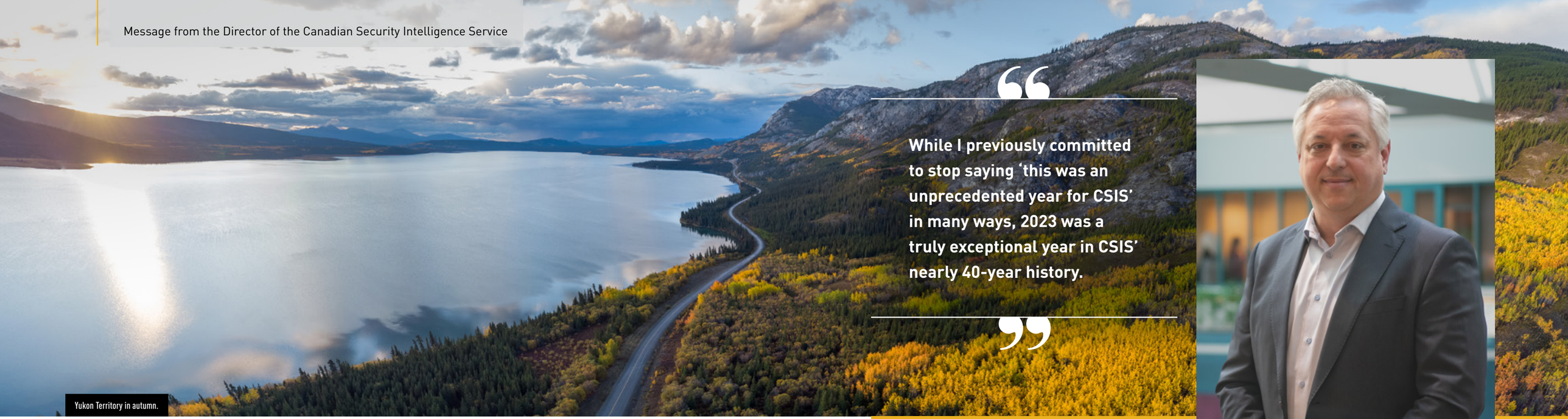
In October, Israel suffered the worst terrorist attack and hostage taking in its history after Hamas attacked Israeli civilians and members of its armed forces. Israel responded to the attack with the launch of an air campaign and ground invasion of Gaza that has had devastating consequences for the local population. In response, Hezbollah and Houthi rebels, backed by the Islamic Republic of Iran, launched missile strikes, raising tensions in the region.

Ongoing conflicts in Ukraine, in the Middle East, and elsewhere remind us that these hostilities are not abstract. Spikes in racism, antisemitism, Islamophobia and acts of hatred here in Canada remind us that our country is not immune. In the fall of 2023, I had the chance to meet with Special Representative on Combatting Islamophobia, Amira Elghawaby, and Special Envoy on Preserving Holocaust Remembrance and Combatting Antisemitism, Deborah Lyons, to discuss the important work we must do to combat Islamophobia, antisemitism, and all forms of hate.

In December, the Royal Canadian Mounted Police (RCMP) arrested an Ottawa youth who was planning a terrorist attack on the local Jewish community. CSIS' efforts had a crucial role in preventing the attack.

Hostile state actors such as the People's Republic of China (PRC), the Russian Federation, and the Islamic Republic of Iran continued to undermine Canada's security, with sustained threat activities, including foreign interference, malicious cyber activities, and economic espionage against Western states.

In October, I participated in the Emerging Technology and Securing Innovation Security Summit at the Hoover Institution at Stanford University with my colleagues from the Five Eyes (FVEYs) domestic intelligence services (FBI, MI5, ASIO and NZSIS). The historic event marked the first time the FVEYs heads met together in a public forum with members of the media, academia, and the private sector from across the FVEYs countries in attendance. The Summit's objective was to alert civil society to the pernicious economic espionage activities of hostile state actors, such as the PRC, that steal billions annually in technology and research from FVEYs economies.



Yukon Territory in autumn.

While I previously committed to stop saying 'this was an unprecedented year for CSIS' in many ways, 2023 was a truly exceptional year in CSIS' nearly 40-year history.

In today's ever-evolving threat environment, security partnerships of like-minded democracies are a necessary and vital factor in combatting the malign activities of authoritarian states. However, national security encompasses more than just governments. It involves every single one of us in our daily lives: the entrepreneur who seeks to sell their software to the world, only to have their intellectual property stolen through economic espionage; the activist who speaks out about human rights abuses in specific countries and is then targeted by regime-directed agents; and the patient who loses vital access to healthcare in a cyberattack targeting hospitals. Whether we know it or not, national security affects everyone; and all Canadians need to play a role in protecting it. National security is a shared effort, built on trust and transparency.

In the fall of 2023, CSIS and the Government of Canada launched a public consultation on its founding legislation, the *CSIS Act*. The threat environment facing Canada is in a constant state of evolution, and Canada needs to ensure that it has the tools necessary to detect and address national security threats. The consultation was a contribution to the national discussion on threats to Canada's security. The proposals for amendments seek to enhance CSIS' authorities to better equip itself to address the threats of today, and the threats of the future. I am pleased to announce that the input received was overwhelmingly positive, which reflects the growing awareness of national security matters by Canadians and the significance they attach to them.

In November, an allegation of inappropriate behaviour in the workplace, reported in the media, was not taken lightly. After the conclusion of an internal investigation concerning serious allegations emanating from CSIS' British Columbia office, CSIS committed to the establishment of an independent ombuds office. Its mandate is to provide an informal mechanism for employees to discuss workplace issues and to act as a supplemental approach to our existing internal processes. In addition to the creation of the ombuds role, I also committed to publishing an annual report outlining incidents of harassment and wrongdoing at CSIS to ensure Canadians can hold us accountable. We are determined to address any such allegations as they are brought to our attention, and in doing so, create a workplace that is respectful, safe, inclusive, and ensures our valued employees can continue to protect Canada and Canadians.

The year 2023 presented significant challenges, and CSIS employees stepped up during this extraordinary year to meet them while truly representing the best of Canada. I am tremendously grateful for their tireless efforts and dedication to the protection of Canada's national security, prosperity, interests, and most importantly, people.

One Mission. One CSIS. One Canada. ■

David Vigneault
Director of the Canadian Security Intelligence Service

National Security in 2023

CSIS investigates activities that may on reasonable grounds be suspected of constituting a threat to the security of Canada.

January

CSIS addresses questions related to PRC foreign interference in the media.

March

Director Vigneault and CSIS officials testify at the Procedure and House Affairs Committee on foreign election interference.

May

Release of the Interim Report of the Independent Special Rapporteur on Foreign Interference.

Ministerial Directive on Threats to Parliamentarians directs CSIS to share more threat-related information with members of Parliament.

The University of Waterloo ceases research with Huawei.

July

Arrest of ideologically motivated violent extremist propagandist Patrick MacDonald, or 'Dark Foreigner.'

Two Canadian extremist travellers arrested upon return to Canada.

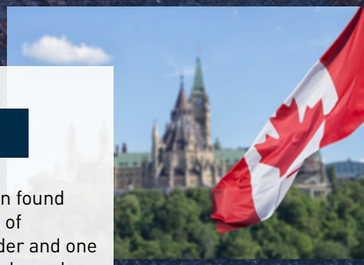
The *One Vision 3.0* Framework on CSIS & RCMP cooperation publicly shared for the first time.

September

Justice Hogue appointed as head of the Public Inquiry into Foreign Interference.

Business Council of Canada report calls for a new national security strategy.

Prime Minister Justin Trudeau makes statement in the House of Commons regarding the murder of Hardeep Singh Nijjar.



November

Nathaniel Veltman found guilty of four acts of first-degree murder and one count of attempted murder. In early 2024, a judge determined his actions constituted terrorist activity.

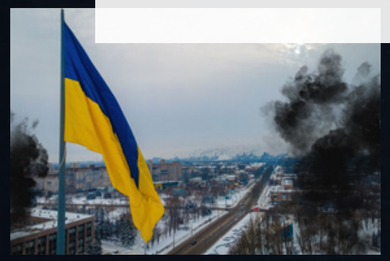
CSIS Act consultations launched.

February

PRC high altitude balloon enters Canadian airspace.

Justice Rouleau issues final report at the Public Order Emergency Commission.

One year since Russia's full-scale invasion of Ukraine.



April

Three Canadian extremist travellers arrested upon return to Canada.

Daesh supporter attack in Surrey, British Columbia.

June

The 2020 Toronto Spa Attack deemed to be an act of terrorism.

Sikh community leader and Canadian citizen Hardeep Singh Nijjar murdered in Surrey, British Columbia.

Arrest of religiously motivated violent extremist Zakarya Rida Hussein and a minor. Two additional minors, part of the same investigation, were arrested in October and December respectively.

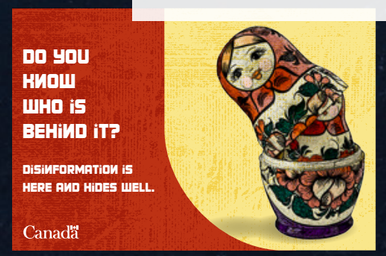
Anti-gender motivated knife attack at the University of Waterloo.

CSIS publishes warning on social media about how the PRC Intelligence Services target and recruit Canadians via LinkedIn.

August

Dominic LeBlanc named Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, and is briefed by CSIS.

CSIS publishes a disinformation awareness campaign on social media.



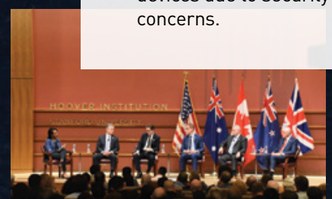
October

Global Affairs Canada releases statement concerning its detection of a malicious information campaign targeting Canadian members of Parliament.

Hamas launches a terrorist attack and hostage-taking in Israel.

Director Vigneault participates in the first ever public appearance of FVEYs leaders at the Emerging Technology and Securing Innovation Security Summit at Stanford University.

The Government of Canada bans WeChat and Kaspersky products on government devices due to security concerns.



December

Arrest of ideologically motivated violent extremists Kristoffer Nippak and Matthew Althorpe.

CSIS Director's Annual Address at the Canadian Human Rights Museum.

Arrest of Ottawa religiously motivated violent extremist planning terrorist attack against the Jewish community.

Federal Court judge denies a PRC national permission to enter and study in Canada due to "non-traditional" espionage concerns.

Highlights

Aurora Borealis

in Yellowknife,

Northwest Territories.

Highlights

MISSION AND PARTNER FOCUSED

Intelligence Reports

In 2023, CSIS produced **2,329** intelligence products

Security Screening

Immigration and Citizenship Screening Program

Requests received in 2023:

493,200

Government Screening Program

Requests received in 2023:

146,000

***Investment Canada Act* (ICA)**

ICA notifications screened in 2022–23 for national security concerns:

1,010

CSIS Partnerships

Domestic Arrangements

91 arrangements with domestic partners

Foreign Arrangements

314 arrangements in **158** countries and territories

CSIS Outreach

In 2023, CSIS conducted **147** engagement activities **30%** more than in 2022

CSIS met with representatives of:

- Indigenous governments and organizations
- Community organizations
- Civil society and advocacy associations
- Research and innovation institutes
- Academia
- Provincial, territorial, and municipal governments

CSIS Briefings to Elected Officials in 2023

Federal 19

Provincial / Territorial 73

Municipal 30

Total 122 **31%** more than in 2022

PEOPLE FIRST

In 2023, CSIS became the **first Five Eyes service to publish its comprehensive Diversity, Equity, and Inclusion (DEI) Strategy.**

Since 2022, CSIS has made progress on **78%** of the commitments within its three-year action plan.

In its inaugural year, CSIS completed **20%** **of the commitments in its 2023–2025 Accessibility Plan.**

ACCOUNTABLE TO CANADIANS

CSIS on Social Media

@csiscanada

Over 9.7 million views on CSIS content in 2023.

157% more than in 2022.

50% increase in total followers across all platforms.

CSIS in the News

Number of articles on CSIS

2023	1,341	118% increase
2022	613	105% increase
2021	298	

Access to Information and Privacy (ATIP)

3,387 ***Privacy Act*** **requests**

172% more than in 2022.

941 ***Access to Information Act*** **(ATIA) requests**

23% less than in 2022.

For the 2023 calendar year, the **on-time compliance rates** stood at

94% for *Privacy Act* requests

92% for ATIA requests

Number of Reviews by National Security and Intelligence Review Agency (NSIRA) and National Security and Intelligence Committee of Parliamentarians (NSICOP)

Ongoing reviews **17**

Completed reviews **2**

Requests for Information (RFI) **300%** more than in 2022.

Parliamentary Appearances

2023	12
2022	13
2021	4
2020	4

1 Mission Focused: Confronting the Threat Environment

Signal Hill from across St. John's Harbour, Newfoundland and Labrador.

CSIS investigates activities that fall within the definition of threats to the security of Canada, as outlined in the *CSIS Act*. Specifically, CSIS is authorized to investigate espionage and sabotage, foreign interference, terrorism and violent extremism, and subversion. Importantly, CSIS is prohibited from investigating lawful advocacy, protest, or dissent, except when it is carried out in conjunction with activities that constitute a threat to the security of Canada.

Duties and Functions

- Investigate activities suspected of constituting threats to the security of Canada, report, and advise on these threats to the Government of Canada.
- Take measures to reduce threats if there are reasonable grounds to believe the security of Canada is at risk.
- Provide security assessments on individuals who require access to classified information or sensitive sites within the Government of Canada.
- Provide security advice relevant to the exercise of the *Citizenship Act* or the *Immigration and Refugee Protection Act*.
- Conduct foreign intelligence collection within Canada at the request of the Minister of Foreign Affairs or the Minister of National Defence.
- Provide assessments by the Integrated Terrorism Assessment Centre (ITAC) that inform the Government of Canada's decisions and actions relating to the terrorism threat.

Pier in White Rock, British Columbia.

Threat Reduction Measures in 2023

Since 2015, CSIS has had the authority to undertake threat reduction measures (TRMs). A TRM is an operational action that is intended to reduce a threat to the security of Canada as defined in Section 2 of the *CSIS Act*. Given its mandate and collection capabilities, CSIS is at times the best placed Government of Canada entity to confront a national security threat. TRMs allow CSIS to take direct actions to diminish a threat to the security of Canada.

These actions fall into three broad categories:

Messaging **Leveraging** **Interference**

All TRMs must comply with the *Canadian Charter of Rights and Freedoms*, and any TRM that would limit a right or freedom, or contravene any other Canadian law, requires a warrant issued by the Federal Court of Canada.

14

non-warranted TRMs in 2023

CSIS' Role in National Security Investigations

While the RCMP and CSIS mandates are distinct, both agencies share an important goal: to address national security threats and ensure public safety. Given CSIS' mandate, it will often have visibility on the emergence of the threat ahead of the RCMP. As established in the One Vision framework, CSIS and the RCMP regularly engage in dialogue to determine the most effective approach to address the threat. If it is determined that a criminal investigation and prosecution is the best approach, both organizations will collaborate in reducing the risk that sensitive CSIS information would be subject to law enforcement's disclosure obligation. In 2023, CSIS information contributed to a number of important arrests in the national security space.

Executive Spotlight – Deputy Director of Operations

Operating in an Increasingly Complex Threat Environment

Vanessa Lloyd, Deputy Director of Operations, is responsible for directing CSIS' human intelligence collection, intelligence analysis, security screening and threat reduction efforts.

I joined CSIS in 1998 as an intelligence officer and have subsequently held operational and supervisory roles where I gained an awareness and appreciation of the breadth of threats facing Canada at home and abroad. Recently, I served as the organization's first Chief Transformation Officer in charge of an ambitious agenda to equip CSIS as a forward leaning intelligence service better able to respond to current and future threats. I was appointed to the position of Deputy Director of Operations in the Spring of 2023, during a significant public discussion on foreign interference threats to Canada's national security. These combined experiences inform my perspectives and current objectives in this role.

I can confidently state that since I joined CSIS, the threat environment has changed significantly. The environment of today is constantly evolving and increasingly complex. Rapid advancements in technology and artificial intelligence now provide hostile state actors and violent extremist organizations alike with capabilities never before thought possible. The proliferation of these technologies and increased volumes of data makes collecting and analysing intelligence in an increasingly digital world a challenge, and make the work of security intelligence professionals harder.

Increased global interconnectivity via the Internet and other digital spaces now allow threat actors outside of Canada's geographic boundaries to influence, co-opt, and radicalize individuals without ever having to leave their country of origin and meet face-to-face. Greater online connectivity means that younger people are increasingly vulnerable to extremist rhetoric and ideas.

Never before have Canada's diverse communities been so highly targeted by such blatant actions of foreign interference. However, this serious threat is not specific to Canada; our closest allies and fellow like-minded countries face the same malicious activities. Hostile state actors have become increasingly belligerent and emboldened to advance their objectives in both the physical and cyber realms, while seeking to silence those who challenge their narrative. They have more options and opportunities to conceal their threat activities, including by using criminal organizations as proxies.

> **Hostile state actors have become increasingly belligerent and emboldened to advance their objectives in both the physical and cyber realms in any way necessary, while seeking to silence those who challenge their narrative.**

Vanessa Lloyd, Deputy Director of Operations at the Canadian Security Intelligence Service.

Canada's adversaries continue to target our talent and intellectual property to advance their espionage and proliferation objectives while national security concerns are increasingly relevant to the assessment of foreign investments in Canada, which could impact our country's prosperity. While the Government of Canada seeks to provide opportunities for new beginnings, security assessments are the first line of defence against the exploitation of immigration pathways by threat actors.

In this threat environment, collaboration and partnerships between international and domestic security intelligence services and law enforcement agencies are more important than ever before in ensuring collective security and increasing CSIS' ability to counter threats from all directions. Canadians can have confidence in CSIS' commitment and ability to collaborate with partners to counter threats to domestic and international security.

How exactly did CSIS respond to the evolving threat environment in 2023? Those answers can be found within this year's Public Report, which is our most comprehensive, threat-focused report released so far. It provides readers with overviews, assessments and awareness of how we protected Canadians and Canadian interests over the past year.

I hope that it will also provide insight into the efforts of CSIS employees who, with dedication and passion, investigate and reduce threats to Canadians and ensure that decision makers are informed of the many threats to Canada's national security. ■

Foreign Interference and Espionage

Foreign interference and espionage activities in Canada continue to be pervasive, sophisticated, and persistent. Active targets of these activities include institutions at all levels of government, private sector companies and associations, universities, civil society groups, and diaspora communities within Canada.

The *CSIS Act* defines foreign influenced activities as "detrimental to the interests of Canada and clandestine or deceptive, or involve a threat to any person." These activities are also commonly called foreign interference and are almost always conducted to further the interests of a foreign state, to Canada's detriment. Malicious interference undermines Canada's democratic institutions and public discourse; and it is used to intimidate or coerce diaspora communities in Canada. That is why it represents a threat to Canada's social cohesion, sovereignty, and national security.

Foreign states engage in a variety of hostile activities such as elicitation, cultivation, coercion, illicit financing, malicious cyber activities, and information manipulation to interfere in Canada.

Major perpetrators of foreign interference and espionage in both Canada and the West include the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and India. In 2023, these states and their intelligence services continued to engage in a variety of hostile foreign interference and espionage activities to advance their objectives and interests.

Foreign Interference Techniques

Elicitation:
Manipulating someone into sharing valuable and sensitive information through conversation.

Cultivation:
Building a strong friendship or relationship with someone to manipulate them into providing favours and valuable information.

Coercion:
Blackmailing or threatening someone to provide valuable and sensitive information or access.

Illicit and Corrupt Financing:
Using someone as a proxy to conduct illicit or corrupt financing on their behalf.

Malicious Cyber Activities:
Compromising electronic devices through various means including socially engineered emails, ransomware, and malware.

Information Manipulation:
Spreading false information on social media to amplify a particular message or provoke users to serve their own interests.

The People's Republic of China

The People's Republic of China (PRC) has one of the world's largest and most active security and intelligence systems. Although primarily focused on ensuring the survival of the Chinese Communist Party (CCP), PRC Intelligence Services (PRCIS) actively carry out clandestine and covert activities targeting democratic states around the world, including the Government of Canada, provincial and territorial governments, Canadian citizens, and Chinese diaspora communities to advance the PRC's national interests. The Ministry of State Security (MSS), China's principal civilian human intelligence service, and other PRCIS apply a variety of methods, including leveraging social media platforms and offering financial incentives to recruit individuals to provide the PRC privileged or classified government or proprietary information. They also attempt to recruit individuals to spy on Canadians whose views challenge the narratives promoted by the CCP leadership.

In 2023, the PRC continued to expand the domestic powers and capabilities of its security services. Under President Xi Jinping, the PRC introduced a suite of national security laws that give its security and intelligence services extra-judicial and extraterritorial powers. These expansive laws elevate the risk of exit bans (a ban to prevent specific individuals from leaving China) or the arbitrary detention of anyone, including foreigners who live, visit, or work in the PRC. These laws also contain provisions, which give the PRC government the ability to control data in China, and to require PRC citizens anywhere in the world to assist and cooperate with China's intelligence services in support of 'national intelligence work.

In 2023, the PRC and its intelligence services continued to harass and intimidate individuals in Canada who speak out against the CCP, thereby undermining fundamental Canadian democratic values. This form of foreign interference can include coercing a victim to return to the PRC or threatening their family members in China. The PRC largely targets those it perceives to pose a challenge to their ruling position, such as human rights activists, political dissidents, journalists, and members of religious and ethnic minority groups. The PRC engages in these activities with a view to shaping local and global narratives on the PRC. These activities can instill fear in affected diaspora communities, silence alternate voices, and trust in government institutions. In addition, the PRC has attempted to apply its National Security Law imposed on Hong Kong in 2020 extraterritorially by issuing warrants and bounties against Hong Kong activists currently in exile, including individuals with ties to Canada.

In addition to normal engagement activity by a foreign government in Canada, the PRC has employed grey-zone, deceptive, and clandestine means to attempt to influence Canadian policy-making at all levels of government (municipal, provincial, federal), Indigenous communities, and broader civil society (e.g., non-government organizations, media, academia, business, cultural). Such activity, which seeks to advance PRC national interests, has the potential to undermine Canada's democratic process and its institutions.

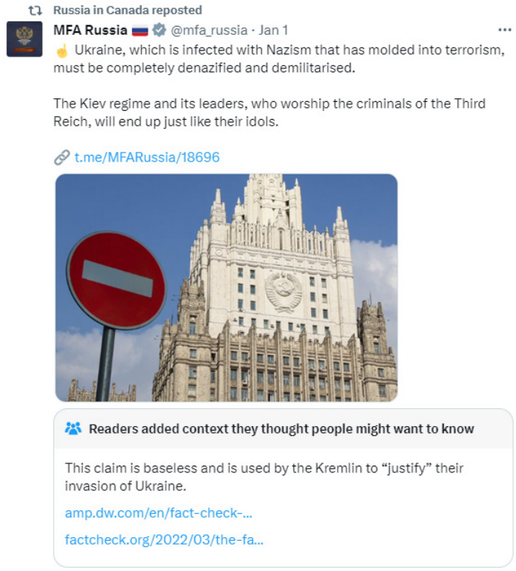
Canada's advanced economy and research expertise makes our country a target of malign PRC activities to advance its strategic, economic, and military interests at the expense of Canadian security and prosperity. The PRC has shown a particular interest in advanced technologies, such as artificial intelligence, quantum computing, biotechnology, and aerospace. The PRC has repeatedly shown that it is willing to use clandestine and deceptive means to acquire intellectual property and advanced technologies from Canada and its allies in order to give PRC companies a competitive and strategic advantage. In addition to traditional espionage, the PRC is actively attempting to recruit Canadians with desirable expertise through social media platforms and talent recruitment firms.

CSIS assesses that the PRC and CCP organizations will remain an enduring threat to Canadian information, technology, democratic institutions, and diaspora communities. The PRC will use a variety of methods, including public engagement, media outreach, and promotional campaigns, as well as deceptive and coercive tactics to affect Canada's behavior and political attitudes in a way that advances its interests. The PRC's negative perceptions of select Canadian domestic and foreign policy initiatives may also drive more foreign interference, disinformation efforts, and cyber activity in 2024.

The Russian Federation

The Russian Intelligence Services (RIS) continue to target Canadians for intelligence collection and collaboration. The RIS continue to be active globally, aiming to collect intelligence and conduct influence operations against NATO allies.

Canada's steadfast support of Ukraine after the Russian invasion in February 2022 continues to make Canada a target for Russian disinformation and foreign interference activities. Russian officials and intelligence services have been actively spreading disinformation as part of a broader campaign to promote their narrative regarding the war in Ukraine, discredit the West, promote Russian influence, and push for an end to Western sanctions. Russia also continues to attempt to discredit Canada's Ukrainian community, falsely claiming that it is composed of neo-fascists who control Canada's foreign policy. Such narratives support the Russian government's efforts to delegitimize and mute the views of Canada's Eastern European diaspora communities and their status as Canadians, in support of Russia's broader hybrid warfare against Ukraine. The Russian Embassy in Canada continues to use its social media accounts to spread disinformation regarding the conflict. Meanwhile, other groups in Canada and elsewhere who receive formal or informal direction from Russian government actors continue to amplify narratives to discredit Canada and its allies' stance on Ukraine via traditional media, social media, and other platforms in the hope of influencing public opinion.



The Islamic Republic of Iran

The Islamic Republic of Iran seeks to be a major power in the Middle East, spreading its influence to Iraq, Syria, Lebanon, and beyond. Its regional ambitions have been advanced primarily through an alliance with Syria and the use of Iran-aligned militias in Iraq, Lebanon, and Yemen. Efforts to obstruct Iran's ambitions by the United States (US), Israel, and other regional states have led Iran to seek informal alliances with like-minded, anti-Western states like the Russian Federation. Iran has formed what it calls the "axis of resistance," a regional alliance of Iran, Syria, Lebanese Hezbollah, alongside other non-state proxy actors. Since the October 7, 2023, Hamas attack against Israel, Iran has publicly praised the militancy targeting Israel and authorized its proxies and allies, including the Houthis in Yemen, to conduct attacks against Israel and US interests in Iraq and Syria. Iran's external operations in Western countries have been increasingly aggressive and expansive in recent years, resulting in numerous disruptions of lethal plots by security and law enforcement services in the US, the United Kingdom and in several European countries. Iran and its intelligence services are interested in influencing and clandestinely collecting information on the Iranian community, including anti-regime activists and political dissidents; human, women's and minority rights activists; and fugitives wanted by the regime. Iran also targets Israeli and Jewish interests as part of its ongoing shadow war with Israel. Iran uses agents, proxies and sympathizers who may be witting or unwitting accomplices. In many cases, the objective is to silence criticism of the regime. In response to this threat, CSIS is actively investigating threats to life emanating from the Islamic Republic of Iran based on credible intelligence, as well as possible precursors to violence including harassment and intimidation from threat actors linked to Iran. Ultimately, these hostile activities undermine the security of Canada and Canadians, as well as Canada's democratic values and sovereignty.

CSIS assesses that Iran will continue to target its perceived enemies even when living in foreign countries in support of its ultimate goal of regime preservation. Iranian threat-related activities directed at Canada and its allies are likely to continue in 2024, and may increase depending on regional developments and the Iranian regime's own threat perceptions.

India

In September 2023, Prime Minister (PM) Justin Trudeau announced to the House of Commons that Canada's security agencies were pursuing credible allegations of a potential link between agents of the Government of India and the killing of a Canadian citizen, Hardeep Singh Nijjar, in Surrey, British Columbia, in early June. The statement led to a deterioration of bilateral relations between Canada and India. Later in November, the US Federal Bureau of Investigation (FBI) unsealed an indictment describing an alleged

murder-for-hire plot by an individual, Nikhil Gupta, whom the indictment alleges was conspiring with a Government of India official. The alleged target was a dual American-Canadian citizen residing in New York.

Prior to the PM's September statement, Director Vigneault and then National Security Intelligence Advisor, Jody Thomas, travelled to India to discuss the matter with their counterparts. In response to the serious allegations, Director Vigneault stated that Canada and its allies require accountability from the Government of India concerning its potential involvement in the murder of a Canadian citizen on Canadian soil.

In January 2024, the Public Inquiry on Foreign Interference requested that the Government of Canada's collection and production of documents include information and documents relating to alleged interference by India during the 2019 and 2021 elections.

Using Social Media to Warn Canadians

In June, CSIS published an advisory to Canadians,[1] warning of PRCIS use of the social networking platform LinkedIn to detect, target, and recruit Canadians located inside and outside of China to engage in espionage. In November, CSIS published a security alert[2] about hostile state actors recruiting Canadian researchers, academics, and experts for dubious international research placements and collaboration opportunities to facilitate economic espionage. In August, CSIS published a disinformation awareness campaign[3] to foster public resilience against disinformation. Together these posts received over one million views across all social media platforms on which CSIS is active, indicating that social media is an effective tool for spreading awareness of hostile state activities targeting Canadians.

CSIS Responds

In 2023, CSIS continued to detect, investigate, and reduce foreign interference and espionage threat activities perpetrated by hostile state actors. Highlighted activities include:

- **Collaborating** with domestic security intelligence and domestic law enforcement partners to respond to and disrupt significant threat activities emanating from the Islamic Republic of Iran, particularly related to the development of lethal capability.
- **Collecting** intelligence and providing advice to the Government of Canada to inform a whole-of-government response against threats to national security.
- **Conducting** nearly 150 engagements with civil society partners to build resilience against foreign interference, espionage, and other hostile state activities.
- **Countering** attempts by the PRC to gain access to Canadian classified and privileged information.
- **Decreasing** the PRC's ability to commit transnational repression through its overseas police stations by working in collaboration with domestic and international partners.
- **Disseminating** intelligence products to Government of Canada partners to increase whole-of-government understanding of the foreign interference and espionage threats targeting Canada.
- **Providing** over 200 security briefings to elected and unelected officials at all levels of government to build resilience against foreign interference and espionage.
- **Meeting** with senior university administrators across Canada to build awareness of the extent of foreign interference activities, such as monitoring, intimidation, and harassment targeting international students on Canadian campuses.

Economic and Research Security

As a global leader in the research and technology sector, Canada is a prime target for foreign states seeking to acquire sensitive research and technologies to advance their own strategic political, economic, and military goals.

In a world marked by economic competition and confrontation, some states seek to advance their strategic political, economic, and military objectives by exploiting investment and trade with Canada. Foreign states seek to acquire access to or control over sensitive technologies, data, and critical infrastructure to advance their own military and intelligence capabilities, deprive Canada of access to economic gains, employ economic coercion against Canada, and support other intelligence operations against Canadians and Canadian interests.

Such activities pose a threat to Canada's national security and long-term economic prosperity.

The *Investment Canada Act* (ICA) sets out a national security review process to mitigate risks and review foreign investments on national security grounds. The national security review process is supported by Public Safety (PS) Canada and Canada's security and intelligence agencies, including CSIS. In 2023, CSIS screened 1,010 ICA notifications for national security concerns.

> Innovation drives our collective prosperity and security, yet the threats to innovation are increasing in both scale and complexity. To meet this challenge, CSIS is working proactively with Five Eyes partners, private sector leaders, and academia to secure our future and to ensure the safety, security, and prosperity of Canada.
>
> **– David Vigneault, Director of the Canadian Security Intelligence Service**

In 2023, CSIS continued to protect Canadian innovation from state actor threats such as targeted investment, coercion, malicious cyber activities, espionage, and the use of collaborative and open research for nefarious purposes. The high-value targets of these threats are expertise, data, and intellectual property.

CSIS contributed to the Government of Canada's research security agenda. To help protect Canadian research and industry, CSIS engaged numerous academic and research associations and companies in the emerging and sensitive technology sectors. CSIS aims to increase awareness of state-sponsored espionage threats targeting these sectors and lay the groundwork for reciprocal partnerships that will help protect Canadian research and development, and ensure Canadians and the Government of Canada have secure access to leading-edge and trusted technology. These briefings were delivered in support of the wider government research security effort, led by PS and Innovation, Science and Economic Development Canada (ISED), which has led to the creation of enhanced security guidelines for research partnerships in Canada.

CSIS worked closely with academic institutions across Canada to share information about national security threats to help safeguard Canadian research and information from economic espionage activities. In 2023, CSIS conducted in-person campus visits to over 13 Canadian academic institutions to engage with senior leadership and administration, faculty, and staff. During these visits, CSIS toured research facilities and laboratories to learn more about the sectors in which the institutions are international leaders to better inform CSIS' ability to protect these complex sectors.

Prioritizing Research Security in the Five Eyes

In October 2023, Director Vigneault participated in the Emerging Technology and Securing Innovation Security Summit hosted by the FBI at the Hoover Institute at Stanford University in Palo Alto, California. The Summit brought together the principals of the domestic intelligence services of the Five Eyes (FVEYs) international intelligence alliance that includes Canada (CSIS), the United States (FBI), the United Kingdom (MI5), Australia (ASIO), and New Zealand (NZSIS) in their first ever joint public appearance. The FVEYs principals were joined by over 450 attendees, including private sector leaders, academics, and journalists. The principals addressed the threats posed to FVEYs economies by foreign states, particularly the PRC, that seek to illicitly acquire the competitive advantage held by FVEYs countries in critical and emerging technologies that include artificial intelligence (AI), quantum computing, and biotechnology.

During the event, the FVEYs principals participated in a discussion hosted by former US Secretary of State, Condoleezza Rice, hosted a press conference with journalists from each respective FVEYs country, and were interviewed for the US television program *60 Minutes*. This historic engagement represents just one of the many steps CSIS and its FVEYs allies took in 2023 to generate greater public awareness of economic espionage threats and reduce its impact within the alliance. ■

Saskatchewan River Delta, Manitoba.

Counter Proliferation

CSIS' counter-proliferation efforts substantially reduce the risk of Canadian technology and products being utilized in the weaponry of adversarial foreign states.

The proliferation of chemical, biological, radiological, and nuclear weapons and their associated delivery vehicles constitutes a global challenge and a threat to the security of Canada and its allies. Several foreign states continue clandestine efforts to procure a range of sensitive, restricted, and dual-use goods and technologies in Canada, as well as expertise they may use to further their own weapons of mass destruction (WMD) programs and delivery vehicles.

CSIS actively investigates efforts by hostile state and state affiliated actors to illicitly procure sensitive technologies and goods in Canada. CSIS also continues to develop its robust understanding of foreign advanced conventional weapons and WMDs, and provide advice to the Government of Canada on sanctions against hostile states.

CSIS activities also include monitoring the development of emerging technologies, and their potential security implications. A prime example is the increasing involvement of private sectors in space technology. Advanced space technology used to be the exclusive domain of states, but due to scientific advancements and private sector capabilities, space platforms, products and services are increasingly available for purchase on the open market.

In its attempt to procure foreign technologies for its war effort against Ukraine, the Russian Federation continues to challenge Government of Canada export controls and sanctions. Russia applies a complex strategy to hide its involvement by falsifying shipping documents and by rerouting shipments through a vast network of intermediaries around the world.

Much like Russia, Iran continues its attempt to evade Government of Canada export controls and sanctions. CSIS engages with Canadian companies to prevent Iran's procurement of technologies that are critical for the development of advanced conventional weapons. This collaboration has helped curb Iran's ability to support destabilizing activities, such as providing weapons to Russia for its war in Ukraine and arming militia groups for attacks against Canadian and partner forces in the Middle East.

Government of Canada Efforts to Mitigate Technology Transfer

In late December 2023, a Federal Court judge upheld the decision by an immigration officer to reject a PRC national's application for a Canadian study permit after concluding that the individual was inadmissible to Canada on security grounds. The officer believed that there were reasonable grounds to believe that the individual could be recruited or coerced by the PRC to engage in espionage activities against Canada or in contrary to Canada's interests. The Chief Justice dismissed the judicial review application brought forward by the applicant in respect to that decision, upholding the decision made by the immigration officer that the applicant could engage in espionage given his expertise in a high priority research area for Beijing (biopharma and advanced medical products) and his association with a Chinese university linked to the PRC's defence industry. These circumstances led both Immigration, Refugees and Citizenship Canada (IRCC) and the Federal Court to conclude that the PRC could utilize the applicant to engage in non-traditional collection activity to facilitate the unauthorized transfer of knowledge and technology from Canada to the PRC. The decision by IRCC and Federal Court is a significant decision in the context of safeguarding Canadian technology and intellectual property from likely applications in the PRC military industrial complex. ■

Cyber Threats

Canada's strong democratic institutions, advanced economy, innovative research sectors, and leading academic institutions make Canada an attractive target for cyber-enabled espionage, sabotage, and foreign influenced activities, all of which pose significant threats to Canada's national security.

CSIS' Role in Cybersecurity

Working closely with trusted domestic and foreign partners, CSIS actively takes steps to investigate and reduce threats to the security of Canada posed by hostile cyber actors, including those in the PRC, Russia, and Iran. To do this, CSIS employs the entirety of its investigative techniques, including the use of dedicated human sources, warranted collection opportunities, and other covert methods. When appropriate, CSIS also takes steps to reduce threats to the security of Canada and Canadian critical infrastructure using its threat reduction mandate.

CSIS routinely provides high-quality intelligence assessments to our government partners, allowing them to make informed policy and operational decisions. CSIS also shares these assessments and investigative leads with our trusted foreign partners in order to assist them in ensuring the integrity of the global information infrastructure, upon which Canadian security relies.

In recent years, CSIS has also assumed a vital public facing role in the cyber domain as it conducts public and private sector briefings in order to alert Canadians to potential cyber vulnerabilities, and help them adopt best security practices. Such efforts help to harden the Canadian cyber ecosystem and reduce the attack surface for hostile actors. Direct briefings to targeted industry sectors, Indigenous groups, and governments, along with presentations and panel discussions at cyber industry and academic conferences, help Canada to remain alert to and resilient in an ever-growing cyber threat environment.

Cybersecurity and Geopolitics

The impact and connection of geopolitics and cybersecurity have become more evident and significant in recent years, as the digital environment has transformed the nature and conduct of warfare, espionage, diplomacy, and trade. Wars are now fought both in the physical and cyber realms. Events like Russia's full-scale invasion of Ukraine and more recently the Israel-Hamas conflict have significantly amplified the need to prepare for the interconnected challenges presented by today's geopolitical and cyber risks.

Throughout 2023, malicious cyber activity targeting Canada continued to increase in scale and complexity, as cyber threat actors sought to advance their economic, political, security, and ideological interests to the detriment of Canada and its allies. Cyber threat actors include state actors operating at the behest of nation-state intelligence services, and non-state actors, both of which aim to exploit weaknesses in information systems or individuals in order to gain unauthorized access to systems and networks. These threat actors are utilizing new technologies such as artificial intelligence (AI) to enhance the sophistication of their cyberattack capabilities.

Canada's cyber threat environment is continuously changing and adapting with the development of new technologies. The constant evolution of the cyber threats targeting Canada demonstrates the need for continued cooperation throughout the Government of Canada and civil society to mitigate this complex and ever-increasing threat.

Information Warfare

Evolving information warfare conducted by hostile states poses an increasingly serious threat to liberal democracies, including Canada. These operations include a range of techniques, but the underlying objective remains the same: to modify the behaviours or beliefs of a targeted audience through the calculated dissemination of targeted information.

Social media is one of the tools used by hostile actors to disseminate disinformation to targeted audiences. While social media disinformation campaigns remain relatively unsophisticated, their effects on demographics of the population should not be taken any less seriously.

Ransomware

Ransomware, a malicious software that restricts access to or operation of a computer or device until a payment is received, continues to be one of the most impactful cyber threats to Canada and Canadians. Ransomware is primarily financially motivated, but states are increasingly leveraging criminal ransomware efforts for their own objectives. Threat actors target those with the largest possible impact, most notably, critical infrastructure, internet technology, and telecommunication systems. Hospitals in Canada were particularly targeted in 2023. While the financial damages have been severe, these attacks also resulted in loss of essential services and widespread loss of extremely sensitive data.

Ransomware is a low-cost tactic that also allows state actors to hide their involvement, as it is still

largely considered to be a cybercriminal tool and law enforcement issue. States likely see value in collecting the intellectual property cybercriminals have stolen and, in some cases, states may perpetrate the activity, with or without interest in the payment, with the intention to obtain a target's data. Leaks of proprietary information and personally identifiable information obtained through ransomware can be used to fuel foreign interference activities like harassment, extortion, and espionage. Such data can provide key pattern of life details, employment history, networks, and more, which can help a threat actor to focus their targeting efforts.

State-based Cyber Threats

The People's Republic of China

PRC state cyber actors continue widespread cyber espionage against a range of sectors and targets within Canada, including government, academic institutions, private industry and civil society organizations. For example, PRC cyber actors have engaged in global mass exploitation campaigns leveraging software vulnerabilities to compromise hundreds of organizations using malicious emails. Every year, cybersecurity researchers discover major vulnerabilities in popular software or hardware products that can be exploited by hostile cyber actors. PRC cyber actors are also active in discovering new vulnerabilities unknown to the public (known as a zero day vulnerability). Even after public disclosure, many vulnerabilities often remain unremedied across all sectors so that even years old vulnerabilities are leveraged by the PRC.

In 2023, cyber actors, allegedly linked to the PRC, employed a network of social media bots to make allegations of criminal and immoral behaviour against Canadian politicians, ultimately attributing the allegations to a Canada-based Chinese-Canadian critic of the CCP. This campaign employed relatively new technologies such as deepfakes demonstrating one of the many ways in which new technology can be leveraged by threat actors.

This past year also saw a major shift in PRC cyber activity, as revealed by a joint FVEYs public disclosure in partnership with the private sector. This activity attributed to the PRC state actor Volt Typhoon, involved the targeting of critical infrastructure sectors in the US that support its military bases. This is the first public indication of the PRC targeting infrastructure of this scale. Sectors targeted ranged from telecommunications, energy, and transportation among others. Disruption in these sectors would impede military operations and have major impacts on civilian populations as well.

Further public disclosures have emphasised the role of compromised Small Office/Home Office (SOHO) devices in facilitating this targeting and the need to harden this type of infrastructure.

The Russian Federation

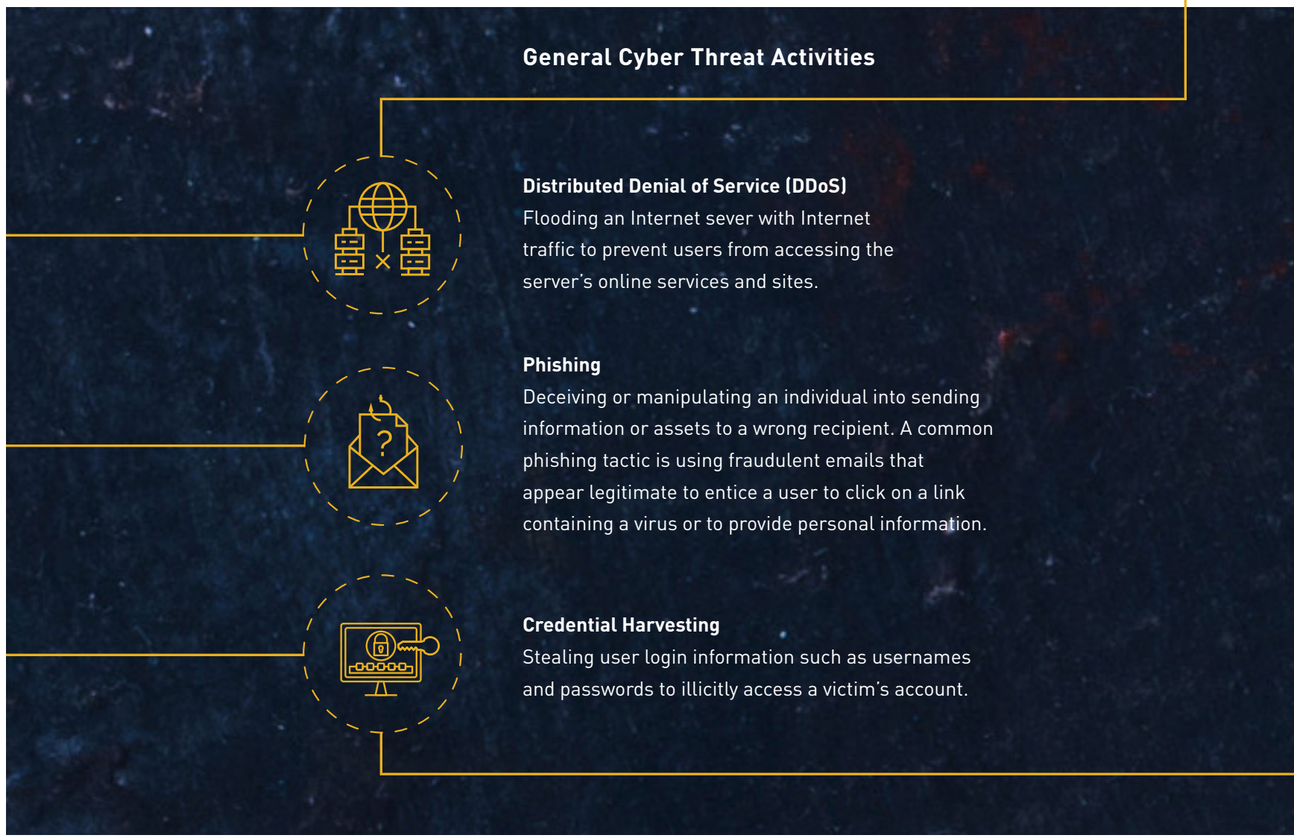
Russia has repeatedly demonstrated intent to display strength by conducting disruptive malicious cyber activities against strategic critical infrastructure targets of their adversaries. Russia also coordinates with non-state groups to conduct cyber threat activity against Ukraine and NATO allies, including Canada. In 2023, pro-Russian cyber actors conducted low sophistication, attention-seeking attacks against Canadian websites. These activities support Russia's hybrid strategy as it aims to intimidate NATO allies and undermine their support for Ukraine. Russia-aligned cyber actors will almost certainly continue to conduct such easy-to-execute, low-cost, deniable cyber activities in the near term against Canada and other NATO allies.

Iran

Iran combines offensive cyber operations with cyber-enabled influence operations to assist in the pursuit of its geopolitical goals. While Canada is not a priority for Iran as compared to the United States and regional Middle East adversaries, most notably Israel, Canada remains a target for opportunistic credential harvesting, phishing attacks, and exploitation of digital infrastructure to facilitate future targeting opportunities against individuals of interest. Iran uses cyber extensively as a tool for the repression and manipulation of critics at home and abroad, including against Canada-based dissidents. Such practices, in combination with Iran's control and manipulation of domestic communications platforms, limit the population's ability to communicate and organize, and serves to uphold the regime's hold on power.

India

Following the deterioration in the bilateral relations between Canada and India, low-sophistication cyber activities against Canada by India-aligned non-state cyber actors were observed. There is no indication that the Government of India was responsible for these cyber incidents.



In response to the many cyber threats targeting Canada in 2023, CSIS continued to work with domestic and international partners to detect and reduce threats to national security. Additionally, CSIS engaged with civil society to build awareness and resilience against cyber threats. ■

Focus on Cyber: Navigating AI Technologies

Rapidly evolving AI technologies present opportunities and challenges to Canada's national security.

The constant evolution of AI technologies has brought the subject to the forefront of conversations across government with private sector, academic, and community partners. AI enables people to work more efficiently by eliminating repetitive and mundane tasks, such as combing through an endless amount of data to search for something in the fraction of the time it would take a human.

In the realm of national security, AI presents both advantages and disadvantages. AI technologies can aid analysts and intelligence officers in their investigation into national security threats. AI capabilities deployed in the right way can be used to detect threats in real time and triage vast amounts of data to look for threat indicators, extremist behaviour, and foreign interference. However, the same advantages offered to CSIS from AI also create vulnerabilities, as both state and non-state threat actors will continue to learn and leverage the capabilities of this technology for malign purposes.

Malicious cyber threat actors are increasingly leveraging generative AI technologies to build and perfect their cyberspace toolkits. AI technologies can be used to conduct malign social engineering activities that facilitate the spread of disinformation online and manipulate targeted audiences towards perspectives or actions aligned with the propagator of the threat. One such technology that presents serious security challenges is deepfakes. Deepfakes are media manipulations, where images, voices, videos, or text are digitally altered or fully generated by AI. This technology can be used to falsely place anyone or anything into a situation in which they did not participate such as a conversation, activity or location.

As Canada's adversaries continue to adopt AI technologies, malicious cyber activities targeting Canadian interests, critical infrastructure, public services, and economic security will only increase.

Developments in AI will make it easier for threat actors to create and propagate disinformation more difficult to identify as false. It is paramount that CSIS and its Government of Canada partners continue to adopt and integrate the technology in a responsible and ethical manner that respects Charter rights to ensure that those who seek to undermine national security and harm Canadians and Canada's interests do not possess an advantage in this critical space. ■

Fredericton, New Brunswick.

Violent Extremism

Violent extremism, whether it is ideologically, religiously, or politically motivated, continues to pose a significant threat to Canada's national security. Monitoring, investigating, and mitigating these serious threats are a key priority for CSIS and its national security community partners.

While only a small number of Canadians are actually willing to engage in extremist violence in support of a cause, as experienced in 2023 and previous years, their actions continue to have devastating consequences on national security. In late 2023, CSIS observed an increase in violent extremist threat activity targeting public safety.

Ideologically Motivated Violent Extremism

The ideologically motivated violent extremism (IMVE) threat is complex, constantly evolving, and fueled by entities (individuals, cells, groups, or networks) driven by a range of influences rather than a singular belief system. Extreme racist, anti-gender and identity, and anti-authority views combined with personal grievances can result in an individual's willingness to incite, enable or mobilize to violence.

Key Ideologically Motivated Violent Extremist Events in 2023

Toronto Spa Attack Ruling: A Historic Decision

On February 24, 2020, a then 17-year-old minor entered the Crown Spa massage parlour in Toronto carrying a sword. He attacked and killed a female employee and injured two other individuals. The minor claimed to be part of the involuntary celibate (incel) community and openly espoused incel narratives. He also allegedly told attending paramedics that he intended to kill everyone in the building, stating, "I'm happy I got one." During an examination of the minor's laptop, police found images of both Alek Minassian, the 2018 Toronto van attack perpetrator, and Elliott Rodger, the ideological founder of the incel movement. The minor claimed that Minassian was an inspiration for his attack.

In late 2022, the minor subsequently pleaded guilty to first-degree murder and attempted murder. At the time, the plea did not include the associated terrorist charges against the accused. Ontario Superior Court judge Suhail Akhtar deliberated on whether the minor's actions met the bar of terrorist activity as defined by s. 83 of the *Criminal Code* of Canada.

In June 2023, Justice Akhtar delivered his ruling, stating that the attack met the *Criminal Code* of Canada definition of a terrorist activity—motivated in whole or in part by incel ideology. On November 28, 2023, the perpetrator was sentenced to life in prison with no chance of parole for 10 years.

The ruling is significant as it provides, for the first time, greater clarity on the meaning of the term 'ideological' and concludes that the incel worldview constitutes an ideology for the purpose of terrorism offences. Further, this is the first time an accused in Canada has been found to have committed "incel-ideologically motivated terrorist activity." Justice Akhtar cautioned, however, that not all incel cases will be crimes of terrorism.

The ruling also clarifies that the definition of terrorism does not require alliance to an organizational or group structure.

What is the incel movement?

The incel movement falls within the 'gender/identity-driven violence' category of IMVE. Involuntary celibates (Incels) are predominantly male online community adherents who define themselves by their inability to engage in sexual activities with women. Incels blame their inability to form sexual relationships on their own perceived genetic inferiority, their belief that women will only ever be attracted to the most attractive men, and perceived oppressive societal structures (e.g. feminism and political correctness). They blame women—and society as a whole—for their personal circumstances.

The Waterloo Attack: An Act of Anti-Gender Driven Violence

On June 28, 2023, Geovanny Villalba-Aleman, a 24-year-old recent University of Waterloo graduate, entered a Gender Studies class on campus and stabbed a professor and two students with a kitchen knife. He was subsequently charged with 11 offences including attempted murder and aggravated assault. On August 31, 2023, the prosecution announced its decision to prosecute Villalba-Aleman as a terrorist.

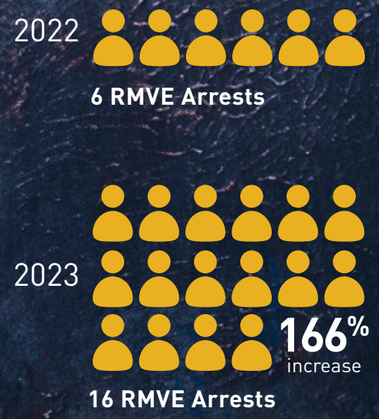
The attack appears targeted and while Villalba-Aleman held various ideological grievances, his primary motivation was likely his anti-gender views. The alleged perpetrator's actions appear driven by a desire to express his grievances and send a message to his perceived enemies. CSIS assesses that the

What is the anti-gender movement?

The anti-gender movement falls within the gender/identity-driven violence category of IMVE and is defined as the ideological opposition to the socio-cultural shifts that are represented by the integration and acceptance of gender theory, including acceptance of the 2SLGBTQIA+ community.

Individuals may become engaged with the movement for many reasons, including beliefs stemming from misogyny, homophobia, transphobia, religious interpretations, conspiracy theories, or a generalized fear of socio-cultural change. While the movement may collectively hold extreme views, CSIS assesses that only a small portion of adherents are willing to engage in serious violence.

Ideologically Motivated Violent Extremism



Canadian Extremist Travellers

- Canadian extremist travellers (CETs) are individuals with an attachment to Canada through citizenship, permanent residency, or a valid visa and are suspected of having travelled abroad to engage in terrorism-related activities.
- The current threat posed to Canada by CETs is religiously motivated.
- CSIS is aware of a small number of Canadians who aspire to travel to join RMVE groups in the Middle East, Afghanistan, and Africa.
- In 2023, six Daesh-affiliated CETs and their children returned to Canada from internally displaced persons camps in Syria.

attack constitutes an act of IMVE and represents an example of anti-gender ideology violence.

CSIS assesses that the violent threat posed by the anti-gender movement is almost certain to continue over the coming year and that violent actors may be inspired by the University of Waterloo attack to carry out their own extreme violence against the 2SLGBTQIA+ community or against other targets they view as representing the gender ideology agenda.

While violent rhetoric itself does not equate or often lead to violence, the ecosystem of violent rhetoric within the anti-gender movement, compounded with other extreme worldviews, can lead to serious violence. CSIS assesses that exposure to entities espousing anti-gender extremist rhetoric could inspire and encourage serious violence against the 2SLGBTQIA+ community, or against those who are viewed as supporters of pro-gender ideology policies and events.

Major Ideologically Motivated Violent Extremist Arrests

On July 5, 2023, the RCMP arrested Patrick Gordon MacDonald, an Ottawa-based creator and propagator of neo-Nazi IMVE propaganda material. MacDonald produced graphic propaganda material under the alias 'Dark Foreigner' and had influence in the international neo-Nazi violent extremist movement. The Ottawa man was charged with participating in the activity of a terrorist group, facilitating terrorist activity, and commission of an offence for a terrorist group. In its statement, the RCMP commented that MacDonald's arrest represented the first time in Canada "in which an individual advocating a violent far-right ideology has been charged with both terrorism and hate propaganda."

On December 6, 2023, the RCMP arrested two Ontario men, Matthew Althorpe and Kristoffer Nippak, on terrorism charges for their alleged participation in the creation of manifestos and recruitment videos in support of the international neo-Nazi movement. Both men are alleged to have participated in the creation of Terrorgram collective manifestos and Atomwaffen Division recruiting videos. The Terrorgram collective is a group of online channels containing neo-Nazi ideology and manuals for carrying out racially-motivated violence, while the Atomwaffen Division is a listed neo-Nazi terrorist entity in Canada, Australia, and the United Kingdom that calls for violence against racial, religious, and ethnic groups among others to facilitate the collapse of society. CSIS provided the RCMP with assistance throughout this specific investigation, and CSIS intelligence was instrumental in leading to this outcome.

Politically Motivated Violent Extremism

Politically motivated violent extremism (PMVE) encourages the use of violence to establish new political systems or new structures or norms within existing systems. The most notable PMVE event of 2023 was Hamas' October attacks and hostage-takings in Israel, which resulted in the killing of over one thousand people, including seven Canadians. The attack and ensuing conflict have attracted the attention of violent extremists and violent extremist organizations (VEOs) across the globe, and has led to an increase in antisemitic and Islamophobic hate crimes in Canada.

Religiously Motivated Violent Extremism

Religiously motivated violent extremism (RMVE) encourages the use of violence as part of a spiritual struggle against a perceived immoral system. Like other terrorist movements, RMVE actors utilize violence to intimidate or compel a desired action, or to restrain a government from taking an action.

The year 2023 saw the elimination of several key Daesh figures, including a former Caliph and individuals involved with planning terrorist attacks in Europe. While the removal of these key figures is an important factor in countering Daesh's objectives, their deaths have no bearing on the group's ability to inspire attacks. In April 2023, Daesh supporter Abdul Aziz Kawam was arrested for a stabbing attack on a bus in Surrey, British Columbia, and now faces four terrorism charges. More recently, Daesh supporters carried out attacks in Europe in October and December after Daesh called for violence in response to Quran burnings in Western countries. CSIS assesses inspired attacks across the globe will continue during 2024, at an unpredictable

pace, related in part to world events, Daesh messaging, and the individual motivations of the attackers involved.

In 2023, the RMVE threat to Canada increased, as demonstrated by the rise in number of arrests in 2023. Domestic RMVE actors, primarily individuals or small groups inspired by Daesh, Al Qaeda (AQ), or the Israel-Hamas conflict can mobilize to violence quickly. These RMVE actors prefer to use low-sophisticated means against soft targets: a person or group, place, or thing that is easily accessible to the public and generally left unprotected.

In June, Zakarya Rida Hussein was arrested and accused of posting a Tiktok video that contributed to or facilitated terrorist activities for AQ and Daesh. Three minors, part of the same national security investigation, were arrested on terrorism-related charges, respectively in June, October and December. In December, Hussein pled guilty to one terrorism charge related to online recruitment for an attack planned during Pride month.

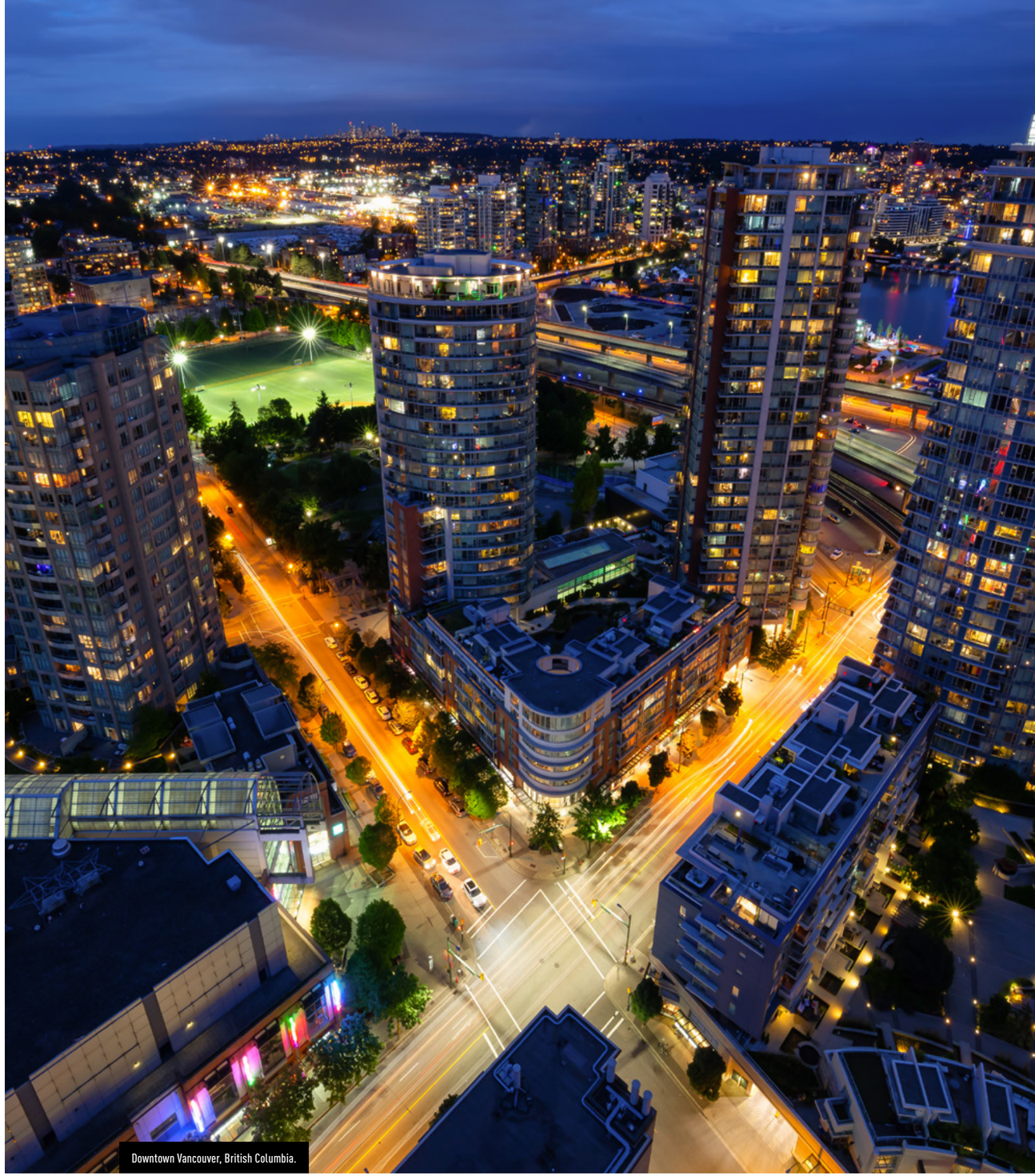
Anti 2SLGBTQIA+ and antisemitic rhetoric is spreading widely through social media and online forums among domestic RMVE adherents, increasing the risk of extremist violence against these communities, and placing youth vulnerable to RMVE propaganda at a higher risk of becoming radicalized on online platforms. Charismatic RMVE leaders in Canada continue to use international events to amplify their propaganda to radicalize and recruit vulnerable individuals while encouraging both domestic acts of violence and international travel to conflict zones. Consequently, CSIS assesses that RMVE actors will continue to pose a domestic threat to Canada in 2024.

CSIS assesses that RMVE is undergoing a generational shift that challenges conventional radicalization and mobilization pathways. Recently, there has been an increase of violent extremists holding highly personalized and at times contradictory ideologies, which they use to justify their acts of violence. Anonymous, permissive online environments have effectively lowered the age-related and societal gatekeeping barriers to extremism, such as parents and educators. RMVE supporters are currently the youngest in modern history, and a shift to leaderless, online radicalization has likely contributed to the development of the hybrid violent extremism ideological trend observed with today's RMVE.

Working in Partnership to Reduce the Violent Extremism Threat

CSIS continued to investigate the national security threat posed by violent extremism in 2023. For obvious reasons a majority of CSIS' counter-terrorism operations must remain classified, however, CSIS was integral to the RCMP's December arrest of an Ottawa youth who planned a terrorist attack in the nation's capital. CSIS is proud to have contributed to this successful outcome, which prevented a potentially significant loss of life.

In response to the ongoing domestic and international threat posed by violent extremists, CSIS will continue to investigate and reduce the threat activities of extremists in collaboration with security intelligence and law enforcement partners to protect public safety. ■



Downtown Vancouver, British Columbia.

Security Screening

Through its Government Security Screening and Immigration and Citizenship Screening programs, CSIS serves as the first line of defence against those who could threaten Canada's national security by obtaining access to Canadian government information, research and data, or by seeking status in Canada via an immigration process.

As part of an overall evaluation to assist federal government departments and agencies in deciding to grant, deny or revoke security clearances, the CSIS Government Security Screening (GSS) program provides security assessments to help prevent individuals of concern from gaining access to classified or sensitive information, as well as sensitive sites such as airports, marine and nuclear facilities. The decision to grant, deny or revoke clearances ultimately rest with each department or agency, and not with CSIS. In 2023, CSIS received 146,000 requests for GSS.

The CSIS Immigration and Citizenship Screening (ICS) program provides security advice to the Canada Border Services Agency (CBSA) and Immigration, Refugees and Citizenship Canada (IRCC) regarding persons who may represent a threat to national security and are attempting to obtain entry to or status in Canada. In 2023, CSIS received 493,200 security screening referrals from IRCC and CBSA. IRCC takes CSIS' advice into consideration when making a final decision on the inadmissibility of an applicant.

The Government of Canada has committed to the security screening of all adult asylum claimants. The volume of in-Canada asylum claimants (also known as Front End Security Screening) has rapidly increased over the last five years and continues to grow every year, creating pressures at ports of entry and leading to delays in process and other strains on the asylum system.

CSIS has played an integral role in the Canadian government's humanitarian effort to resettle, in Canada, 40,000 Afghans fleeing conflict in Afghanistan. In the latter part of this effort, the focus of CSIS' Afghanistan security screening program was on Afghans temporarily residing in Pakistan. This effort was defined by considerable urgency due to Pakistan's stated intention of arresting or deporting (back to Afghanistan) thousands of displaced Afghans.

In early 2023, the federal government agreed to repatriate six Canadian women and their children whom Kurdish authorities had been holding in internally displaced persons camps, in Syria, owing to suspected membership in Daesh as Canadian extremist travellers (CETs). CSIS provided advice on the security threats posed by CETs and collaborated with the RCMP and the Public Prosecution Service of Canada in laying charges and peace bonds on returnees to mitigate potential threats to national security. In addition to the Canadian women, there were also non-Canadian mothers with Canadian children in these camps. CSIS' immigration security screening team took an active role in assessing the risk that the non-Canadian women may pose to national security if granted Canadian status.

In late 2023, the intense fighting between Israel and Hamas raised the prospect of broader crisis in the Middle East. In response, the Government of Canada implemented measures to help Canadians and family members get to safety, including through assisted departures via the Rafah border crossing between Gaza and Egypt. CSIS has been engaged in vetting foreign nationals with ties to Canada who are escaping the conflict. ■

Immigration and Citizenship Screening Program

2023	REQUESTS RECEIVED*
21,600	Permanent Residents Inside and Outside Canada
128,900	Refugees (Front-End Screening**)
296,300	Citizenship
46,400	Temporary Residents
493,200	**TOTAL**

Government Screening Program

2023	REQUESTS RECEIVED*
64,300	Federal Government Departments
8,100	Free and Secure Trade (FAST)
55,300	Transport Canada (Marine and Airport)
2,800	Parliamentary Precinct
10,400	Nuclear Facilities
100	Provinces
600	Foreign Screening***
1,900	Special Events Accreditation
2,500	Others
146,000	**TOTAL**

*Figures have been rounded.

**Individuals claiming refugee status in Canada or at ports of entry.

***Security assessments to provincial and foreign governments, as well as to international organizations, when Canadians seek employment that requires access to sensitive information or sites in another country.

Integrated Terrorism Assessment Centre

The Integrated Terrorism Assessment Centre leverages all-source data, information and intelligence to deliver timely, rigorous and objective assessments that enable decision makers and security partners to safeguard Canadians and advance Canadian interests.

The Integrated Terrorism Assessment Centre (ITAC) is a both a functional analytical component of CSIS and a community resource. It operates under the provisions and authorities of the *CSIS Act*.

Integrated analysis is most pertinent to national security decision-makers in complex times. Today, intense intersections exist between terrorism, polarizing social issues, great power competition, food insecurity, and technological innovation.

ITAC strives to meet the needs of a range of clients, including the federal government, law enforcement and infrastructure partners through timely assessments published at multiple levels of classification. In 2023, ITAC received ministerial direction to begin assessing all national security threats to public officials.

2023 Trends and Looking Ahead

Following a surge in ideologically motivated violent extremism (IMVE) in 2022, and at the end of 2023, a rise in the prevalence of religiously motivated violent extremism (RMVE), ITAC assesses that an IMVE and a RMVE attack is equally likely to occur in Canada in 2024. In response, ITAC will continue to support departments responsible for risk mitigation measures.

A 2023 trend that will continue into 2024 concerns violent rhetoric and criminal activity targeting the 2SLGBTQIA+ community, Jewish and Muslim communities, public officials, and democratic institutions in Canada. ITAC assesses that the volume of online threats and violent propaganda propagated in 2024 will be exacerbated by conflict in the Middle East.

Over the course of 2023, the National Terrorism Threat Level remained at Medium, meaning that a violent act of terrorism could occur in the next 12 months. Canada has been at Medium since 2014.

Going into 2024, ITAC looks forward to celebrating its 20th anniversary and to continuing to provide services to safeguard Canadians and advance Canadian interests at home and abroad. ■

ITAC's four lines of effort

1. Reporting on terrorism threats, trends and events.
2. Assessing and recommending the National Terrorism Threat Level for Canada.
3. Assessing and setting terrorism threat levels for Canadian interests worldwide, including for special events and internationally protected persons.
4. Developing strategic all-threat assessments for public officials.

North of Moose Jaw, Saskatchewan.

2 Partner Focused: Engaging with Canadians and Partners

Angus L. Macdonald

Bridge at twilight.

The span connects

Halifax and Dartmouth,

Nova Scotia.

Executive Spotlight – Deputy Director of Policy and Strategic Partnerships

Shining the Light: Building a Strategic, Transparent, and Accountable CSIS

Nicole Giles, Senior Assistant Deputy Minister and Deputy Director of Policy and Strategic Partnerships, is responsible for strategic policy development, legislation, and strengthening key partnerships and engagement with oversight bodies, the Government of Canada, foreign partners, and all Canadians.

I joined CSIS in late 2022, having spent my career working on international issues for the Government of Canada, both In Canada and as an ambassador abroad. Everyday I apply these experiences, including my time spent in academia, to help strengthen CSIS and Canada's national security.

Our mandate in the Policy and Strategic Partnerships Directorate is simple: facilitate the mission. To achieve this key objective, the Directorate ensures that CSIS is well positioned to strategically guide and respond to all complex policy and operational matters affecting its day-to-day activities. It also acts as CSIS' most prominent advocate in engagements with government partners, Parliament, provinces and territories, Indigenous governments, community organizations, and the Canadian public, our most important partner. As part of our strategic approach we have established three critical priorities: strategy, transparency, and accountability.

First, we must ensure that CSIS has a strong framework that guides the implementation of Government of Canada policies and legislation through a whole-of-CSIS response, from operations to policy. This also allows CSIS to collaborate more effectively with Government of Canada partners on issues of national security.

One recently developed key strategic framework is CSIS' Indo-Pacific Strategy (IPS) Framework. The CSIS IPS Framework builds upon the broader Government of Canada strategy for the region and guides all CSIS activities in the region. Under the IPS, we are increasing engagement and expanding our relationships with key regional partners, which in turn allows us to better respond to threats and hostile activities emanating from the region to better protect Canada's national security and economic prosperity.

Grands-Jardins National Park, Charlevoix, Quebec.

Another key strategic framework is our Northern and Arctic Framework, which guides CSIS' implementation of the *United Nations Declaration of the Rights of Indigenous Peoples Act* (UNDA). In 2023, CSIS made history as the first intelligence service in the world to action the UNDA declaration. This important framework based on reconciliation and cooperation will guide CSIS as it expands and strengthens its relationship with Indigenous governments, organizations, communities and peoples, all of whom have an integral role to play in protecting national security.

Strategic frameworks guide all CSIS engagements. In October, I travelled to Iqaluit to discuss building stronger relationships and collaboration on security matters with the Government of Nunavut and other key Arctic partners. During a sitting of the Nunavut Legislature, I was honoured, on behalf of CSIS, to be officially recognized by Premier P.J. Akeeagok, who thanked CSIS for its ongoing engagements with regional partners and enhanced prioritization of Arctic and Northern Security. Engagement and communication is key to building strong partnerships and trust between all Canadians and their security intelligence service.

Transparency remains one of our utmost priorities. As such, we endeavour to ensure CSIS is as transparent as possible with Canadians concerning its important work in protecting national security while ensuring the continued protection of sources of intelligence and CSIS methodologies. It is time for CSIS to not only come out of the shadows, but to be the one shining the light. Canadians may have noticed in recent years that CSIS has been more publically engaged than ever before. This is evident through our recent public acknowledgements of CSIS' critical efforts in major national security investigations; our increased engagement with the media; our public release of our comprehensive Diversity, Equity, and Inclusion (DEI) Strategy; and through key public products like this public report, which for the first time features key CSIS executives.

Even for a security intelligence service, transparency is relevant and essential, particularly if we want to build

trust with all those we serve. It ensures that Canadians have a better understanding of what we do, which leads to a more informed discussion on national security and ultimately builds their resilience against threats. This is why we decided to publish operational statistics in this year's public report, which can be found on pages 25 and 67.

True accountability must be built on a foundation of transparency brick by brick, which is the third priority. Being accountable to Canadians and Parliament is paramount to earning and maintaining trust, which is why we prioritize our relationships with external bodies like the National Security and Intelligence Review Agency (NSIRA), the National Security and Intelligence Committee of Parliamentarians (NSICOP), the Federal Courts, and the Intelligence Commissioner. We welcome the reviews these bodies conduct of CSIS activities and their recommendations because we are a learning organization that constantly strives to improve. In 2023, we experienced a 300% increase in requests for information and briefings, which were actioned to ensure review bodies received the necessary information required to conduct a thorough review. To further transparency and accountability, CSIS began to provide public responses to these recommendations to ensure Canadians are aware of CSIS' position on specific matters and the actions we will take to address them.

Another key accountability and transparency mechanism is realized through parliamentary appearances. In 2023, CSIS executives, including myself, provided testimonies to various parliamentary committees on topics ranging from research security and foreign election interference.

Effectively facilitating the mission requires that CSIS be strategic, transparent, and accountable. Building trust and strong relationships takes time. Canadians have historically been unaware of their security intelligence service and how we protect them; going forward, that must change. As we enter into an increasingly complex threat environment, CSIS must be better positioned to effectively respond and counter these threats, and Canadians must be more informed on national security concerns. Ensuring the safety, security, and prosperity of Canada requires a whole-of-society effort, and CSIS will continue to include all Canadians in this collective effort. ■

> **"It is time not only for CSIS to come out of the shadows, but to shine the light."**

Nicole Giles, Deputy Director of Policy and Strategic Partnerships at the Canadian Security Intelligence Service.

Rideau Falls, Ottawa, Ontario.

Building Partnerships through Engagement

In recent years, CSIS has prioritized its external engagement activities because combatting whole-of-society national security threats requires a whole-of-society effort.

The world of national security and intelligence has evolved rapidly in the last several years, and accordingly so has the way we work. In service of its commitment to ensuring the safety, security, and prosperity of all people in Canada, CSIS continues to enhance its outreach with civil society. CSIS' strong relationships with community partners, businesses, and academia are crucial to building resilience against national security threats, and earning the trust of Canadians is foundational to that effort.

Academic Outreach

In 2023, CSIS hosted nine virtual expert briefings, produced 17 commissioned reports, facilitated six expert roundtables, and provided expert advice to a number of Government of Canada funding advisory boards working with civil society and community organizations to counter violent extremism.

On May 24, 2023, CSIS hosted its first hybrid workshop since the pandemic to examine the threats posed by deepfake disinformation technologies. The workshop was designed around the work of eight leading experts from across the open-source research community and attended by 130 Canadian and foreign government representatives, and select members of private industry and academia. CSIS published the summary and findings of the workshop in a report titled *The Evolution of Disinformation: A Deepfake Future,* which can be found on the CSIS website.[4]

Partner Engagement

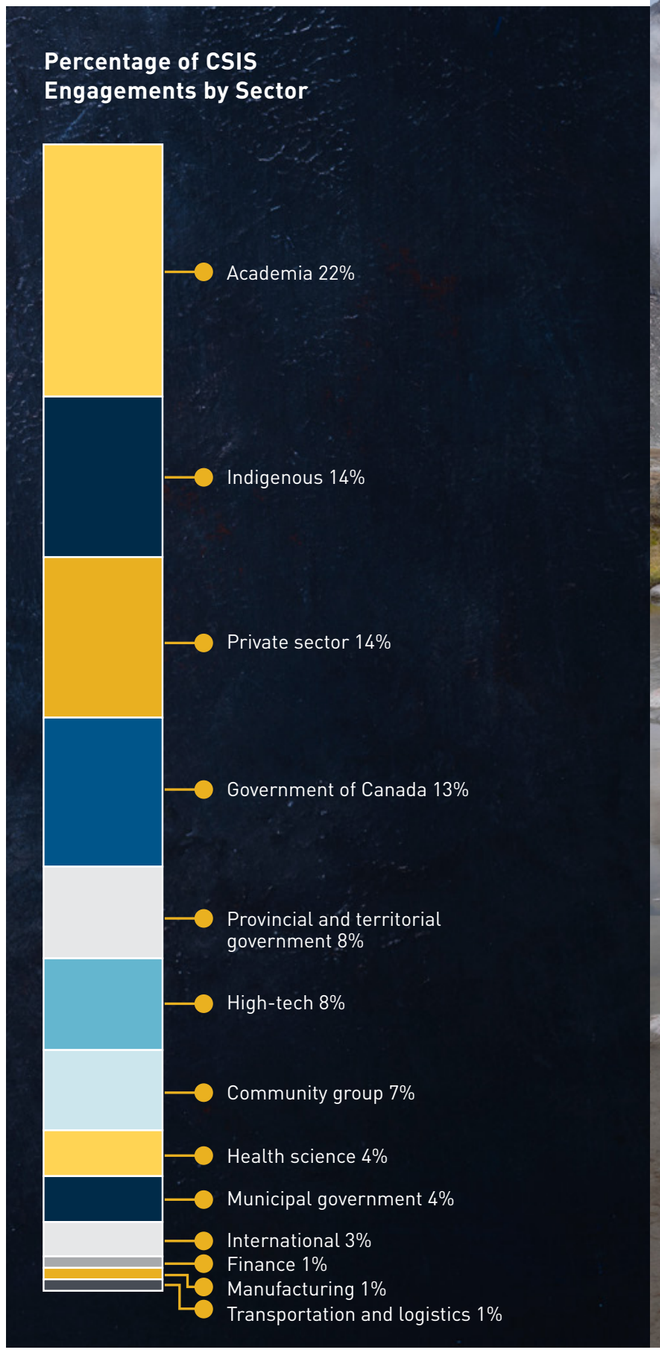
In 2023, CSIS conducted 147 outreach engagements with various partners across multiple sectors. CSIS' outreach engagements aim to develop relationships with, work alongside, and learn directly from Canadians. This year marked several milestones.

In support of securing Canada's Arctic and North, CSIS had numerous engagements with Arctic and Northern partners, including governments, communities, and Indigenous groups. In March, CSIS presented at the Inuit Technology Forum in Iqaluit. The presentation, made available in Inuktitut to the participants, focused on cyber threats to the security of Canada. In November, CSIS, Inuit Tapiriit Kanatami, and the Privy Council Office established a mechanism that supports Inuit leadership in accessing security screening services. This important milestone will facilitate the sharing of information, while supporting Inuit self-determination.

In addition to CSIS' traditional outreach and engagement channels, CSIS senior executives have increased their participation in public-facing events. In 2023, then Assistant Director of Requirements, Cherie Henderson, spoke at the Canadian Security Showcase on the latest developments in the security landscape, and the importance of operational partnerships and exploring future approaches to protect national security.

In September, Director Vigneault gave the keynote address to the members' meeting of the Business Council of Canada (BCC), a network composed of 170 chief executives of Canada's leading enterprises, which together employ millions of Canadians and contribute 50% to Canada's private sector GDP. In his address, Director Vigneault spoke about the targeting of Canadian innovation and industry by foreign state actors, such as the PRC. CSIS' robust relationship with the BCC is a demonstration of CSIS' work to increase resilience against foreign interference in private industry, so that Canadian jobs, technology, and intellectual property are protected. The BCC's 2023 report, *Economic Security is National Security*, is one result of this important partnership.

On December 11, Director Vigneault delivered his annual address at the Canadian Museum for Human Rights in Winnipeg, Manitoba. The theme of his address was the interconnection of human rights and national security. Director Vigneault discussed the increasing complexity and intensity of security threats, CSIS' efforts to uphold and defend human rights and democracy in today's rapidly evolving geopolitical environment, and how a successful response to threats requires working in partnership with civil society. This event marked the first time the Director provided his annual address with journalists in attendance. ■




Akshayuk Pass, Baffin Island, Nunavut.

Policy and Accountability

Protecting national security and Canada's interests requires CSIS to be a policy-driven organization that is accountable to Canadians and Parliament.

The Arctic and Northern Framework

In the Fall of 2023, the CSIS Arctic and Northern Framework was finalized, defining a strategic and coordinated approach to CSIS engagement in the region. The framework applies a comprehensive strategy that will guide CSIS as it strengthens existing relationships with partners, and increases its involvement in the region to help safeguard it from national security threats, such as espionage, foreign interference, and illicit economic initiatives, all of which seek to fundamentally undermine Canada's sovereignty.

The framework applies CSIS' mandate and capabilities to support Canada's security and economic interests, while enhancing domestic resilience to the increased hostile state activities targeting the Arctic and North. Under the framework, CSIS will increase its resources and focus in the region to collect information on suspected threats to national security, support both Government of Canada and non-government partners operating in the region, and mitigate and reduce security and economic threats to governments, communities, and Canada's interests in the Arctic and North.

Indigenous peoples are at the heart of the framework, as they possess critical insight specific to distinct regional security challenges. CSIS will continue to engage and build partnerships with Indigenous peoples, governments, and communities, as their perspectives and support are integral to protecting Canada's Arctic and Northern sovereignty from hostile state actors.

The Indo-Pacific Strategy

In 2023, CSIS continued to implement its landmark Indo-Pacific Strategy (IPS) policy framework, which will guide whole-of-CSIS engagement in the region as it grows its partnerships and engagements with select Indo-Pacific partners and strengthens coordination with Canada's closest allies on common priorities.

Alongside these efforts, CSIS will focus on increasing its capacity to counter threats and hostile activities emanating from the region, including those perpetrated by hostile state actors relating to foreign interference, espionage, cyber, disinformation and misinformation. IPS funding will support sustained investigations into these threats through enhanced collection and analytical capabilities. Additionally, IPS resources will also strengthen CSIS' ability to counter domestic threats. As part of this, CSIS will systematically engage Canadian partners on risks relevant to their increased involvement in the Indo-Pacific, including other government departments, non-governmental organizations, universities, and civil society organizations representing key communities and stakeholders in Canada with a nexus to the region.

Consulting Canadians: *CSIS Act* Consultations

On November 24, the Government of Canada launched consultations on targeted legislative amendments to increase CSIS' ability to counter foreign interference. CSIS, in collaboration with Government of Canada partners, began consulting with Canadians, including community and business groups, academics, and Indigenous governments on proposed amendments to the *CSIS Act*. These consultations and proposed amendments represent the most promising opportunity in recent years to fill critical gaps and support CSIS' ability to operate in the 21st century.

Today's threat environment is markedly different from the threats Canada faced in 1984. This is clearest when we think about threats from foreign interference or advancements in technological capabilities and data analytics. CSIS faces significant challenges as it continues to rely on authorities designed in, and for, a bygone era.

Threat actors can hide in plain sight, spread disinformation, siphon the personal data of Canadians, and influence public discourse. Threat activity often festers in the online space, where widely available tools designed to protect the privacy of Canadians and Canadian companies make threat actors difficult to detect and identify.

To address these concerns, CSIS and Government of Canada partners put forward five major areas that would benefit from amendment to close policy and legal gaps: information sharing, judicial authorizations, dataset collection and use, foreign intelligence collection, and a statutory review of the *CSIS Act*.

The Government of Canada heard from individual Canadians, through an online portal, in addition to holding roundtable discussions with key partners from academia, civil society, and diaspora communities, on how the *CSIS Act* amendments could affect Canada from their perspective. Government of Canada representatives also met with delegations from every province and territory. This feedback informed the Government's reflections on potential changes to key aspects of CSIS' guiding legislation and ensured Canadians understood the challenges facing CSIS legislatively, a comprehension of which is paramount to meaningful change.

External Review and Oversight

Review bodies ensure that CSIS remains accountable to Canadians and compliant with the law and the Charter while conducting its duties to protect all Canadians.

External reviews by the National Security and Intelligence Committee of Parliamentarians (NSICOP) and the National Security and Intelligence Review Agency (NSIRA) provide CSIS with the opportunity to enact positive change in response to recommendations and findings. In 2022 CSIS began providing public responses to review body recommendations to ensure Canadians are aware of actions CSIS plans to take. While not every recommendation is fully accepted, CSIS takes the time to analyse each one and take action on the recommendations with which it fully agrees and are feasible to implement. Independent external review also fosters a culture of compliance and continuous improvements at CSIS through public reports, and help inform Canadians on key national security issues.

CSIS devotes significant attention and resources to requests for information or briefings from review bodies. In 2023, between NSIRA and NSICOP, there were 19 national security reviews involving CSIS. In addition to this, CSIS received 97 requests for information and briefings from review bodies, which represents a 300% increase from 2022 to 2023. CSIS welcomes this level of external review as an investment in ensuring CSIS remains accountable in fulfilling its requirements as Canada's security intelligence service.

In 2023, NSIRA published two reviews involving CSIS, the 2021 TRM review and the 2023 Global Affairs Canada's Global Security Reporting Program review, in addition to two statutory reviews of the *Security of Canada Information Disclosure Act* and *Avoiding Complicity in Mistreatment by Foreign Entities Act* affecting CSIS and a number of other departments and agencies. CSIS is expecting a number of reviews to be published in early 2024, including the reviews on foreign interference in the federal elections by NSIRA and NSICOP commissioned in response to the Prime Minister's request in early March 2023.

The Intelligence Commissioner (IC) provides an additional layer of oversight and accountability for CSIS. The IC reviews decisions of the Minister of Public Safety on classes of datasets, and approves the retention of a foreign dataset under Section 11.17 of the *CSIS Act*, as well as the categories of acts and omissions that designated CSIS employees can commit that would otherwise constitute offences. With the goal of further increasing transparency, the IC publishes decisions on its website, similarly to NSICOP and NSIRA. In 2023, the IC rendered seven decisions, four of which have already been made publicly accessible.

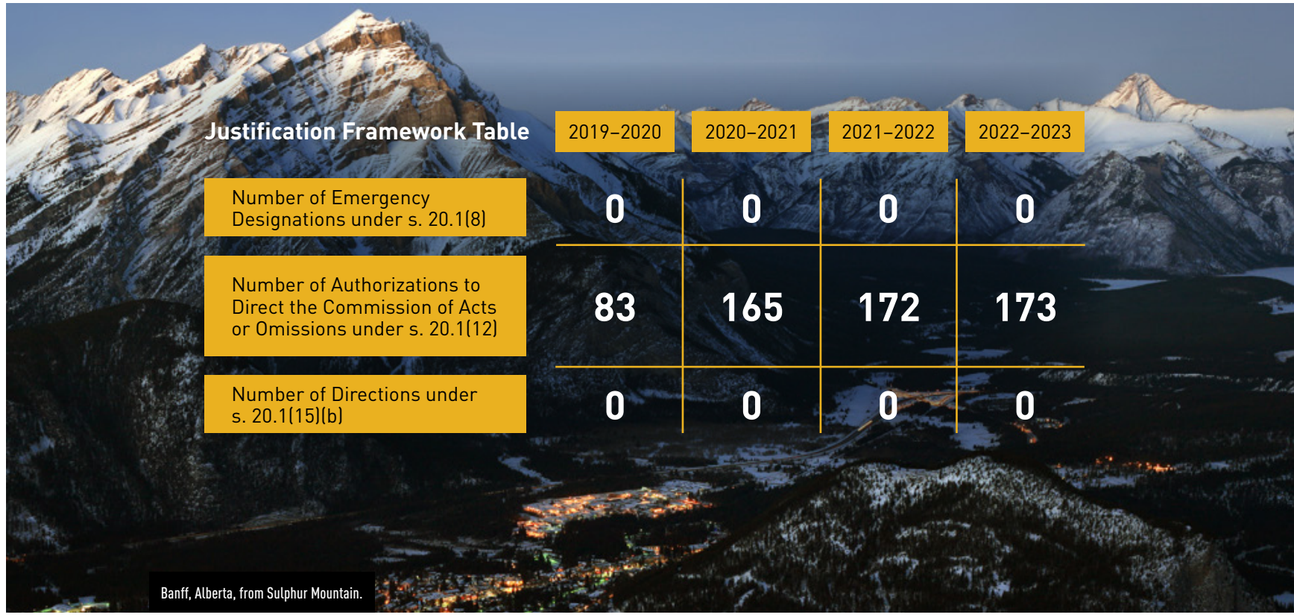
In order to provide a source of expertise and guidance on privacy practices, CSIS has a dedicated privacy unit to respond to the increasing complexity in the privacy landscape. The unit engages with the wider Government of Canada to consult on and discuss the privacy expectations and considerations for Canadians. Further, it ensures continued engagement with the Office of the Privacy Commissioner to determine privacy best practices for the CSIS program, and to ensure conformity with the *Privacy Act.* In the past calendar year, the Privacy Unit has completed the review of seven privacy breaches (two founded, four unfounded, one underway); conducted 17 privacy needs assessments (13 currently underway) and begun drafting five privacy impact assessments.

Justification Framework

The *National Security Act* (2017) acknowledged that it is in the public interest to ensure that CSIS employees can effectively carry out CSIS's intelligence collection duties and functions, including by engaging in covert activities, in accordance with the rule of law. To enable this, the amendments provide a limited justification for CSIS employees and persons acting at their direction to carry out activities that would otherwise constitute offences, modelled on the framework already in place for Canadian law enforcement.

The Justification Framework provides legal authority for CSIS employees who are designated by the Minister of Public Safety and persons acting under their direction, such as human sources, to engage in activities that would otherwise constitute offences. This means that when a CSIS employee, or human source acting at their direction, engages in activities with a suspected terrorist in the hope of gaining their confidence, they are protected from criminal liability. For example, the very act of providing direction to a human source operating covertly within a suspected terrorist entity could potentially engage terrorism offences in the Criminal Code. Another example is providing electronic items, such as a cell phone, to enable the human source's access to vital information.

As a first layer of accountability, the Framework requires the Minister of Public Safety to determine, at least once a year, the classes of acts or omissions that designated CSIS employees may be justified in committing or directing another person to commit, and this determination is only valid after it is reviewed and approved by the IC. As a second layer of accountability, and as an added layer of transparency, Section 20.1(24) of the Justification Framework also requires the Minister to publicly release certain information. The following table provides the information required to fulfill Section 20.1(24), by fiscal year:



Justification Framework Table

	2019–2020	2020–2021	2021–2022	2022–2023
Number of Emergency Designations under s. 20.1(8)	0	0	0	0
Number of Authorizations to Direct the Commission of Acts or Omissions under s. 20.1(12)	83	165	172	173
Number of Directions under s. 20.1(15)(b)	0	0	0	0

Banff, Alberta, from Sulphur Mountain.

Since the coming into force of the Justification Framework, the majority of the authorizations granted were in support of information and intelligence collection activities relating to espionage/sabotage, foreign interference, and terrorism as defined in paragraphs (a), (b), and (c) of the definition of threats to the security of Canada in Section 2 of the *CSIS Act*. During the same time, the majority of the acts or omissions that were directed to be committed under paragraph (b) were related to terrorism as defined in paragraph (c) of the definition of threats to the security of Canada in Section 2 of the *CSIS Act*, and as such could constitute terrorism related offences under the *Criminal Code*. ■

3 People First: A Workplace for All

Vancouver, British Columbia, from Stanley Park at night.

Executive Spotlight – Assistant Director of Human Resources

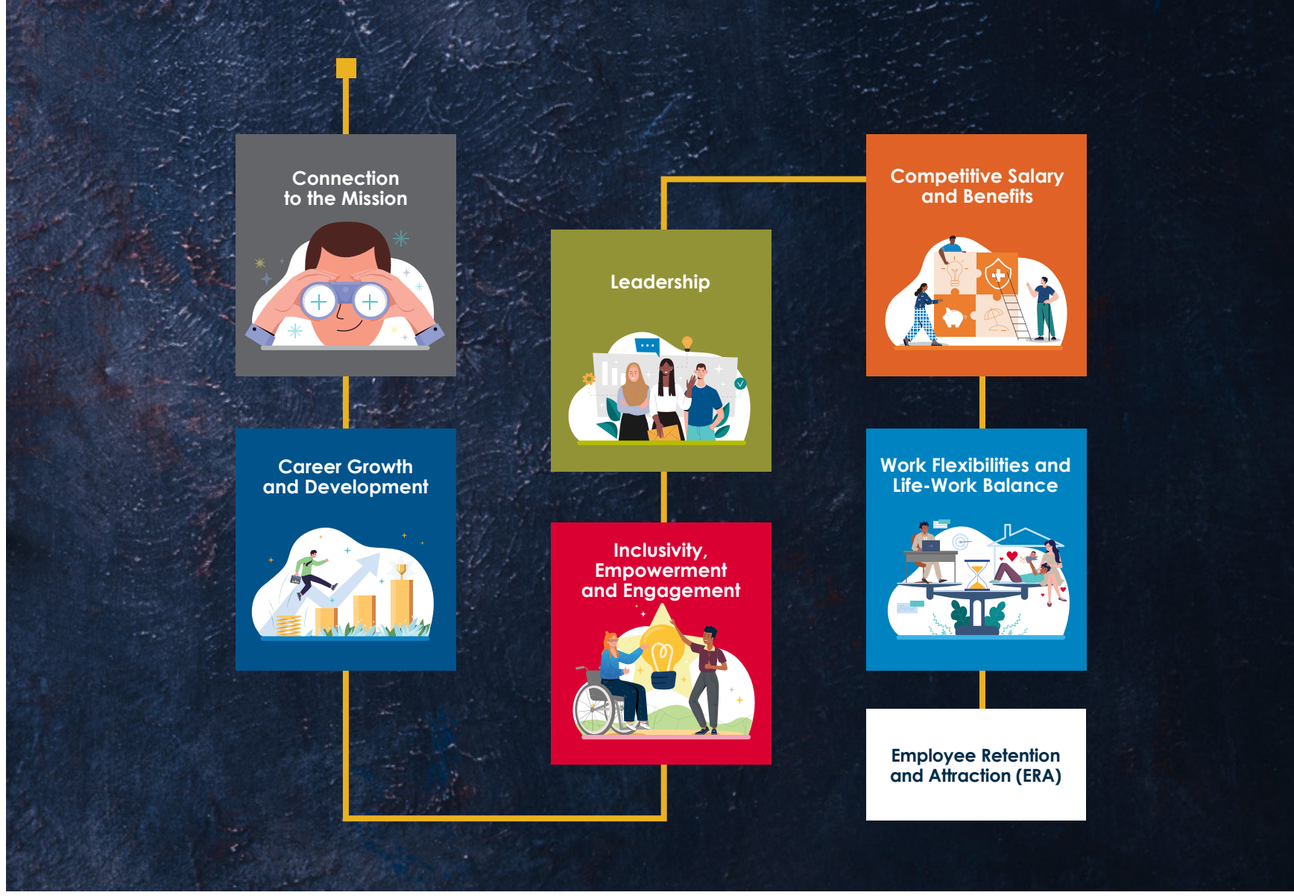
People First: In Pursuit of a Better CSIS

Renée de Bellefeuille, Assistant Director of Human Resources and Chief Human Resources Officer, is responsible for the strategic management of all human resources-related areas at CSIS.

CSIS offers a unique career experience, as the roles all support the mandate to protect Canadians and Canada's national security and interests from threats. However, like any other workplace, CSIS has its challenges concerning hiring and retention, as there are several considerations and sacrifices that come with working in a classified environment. The professional and personal implications of working for CSIS include the impacts of working in a Top Secret environment, including the intrusive screening process, requirements to maintain a security clearance, and identity protections. The restrictions implicating employees' personal lives also include travel limitations and prohibitions of electronic devices, amongst others. Our ability to provide telework options is limited, requiring the vast majority of employees to work on site.

In consideration of these challenges and after extensive consultations with hundreds of CSIS employees across the country, my team and I launched the Employee Retention and Attraction (ERA) plan in late 2023 to transform CSIS into a more people-focused organization while ensuring we continue to support the CSIS mandate and crucial work of all employees. The ERA prioritizes six areas to improve the overall experience of people at work: connection to the mission; career growth and development; leadership; inclusivity, empowerment and engagement; competitive salary and benefits; and greater work flexibilities and life-work balance. We are entering a new era at CSIS, one that places our valued existing and prospective employees first. I am confident that this strategy, through its many timely and necessary changes, will facilitate an improved employer-employee relationship at CSIS that will help us retain and attract great talent.

Canadians who have considered working at CSIS, or are just hearing of us now, should know that a career in security intelligence is highly rewarding. CSIS employees work to protect Canada's national security and safeguard its people and secrets. We offer over one hundred types of positions in support of the mission that range from intelligence collection, analysis, information technology, human resources, finance, and linguistics among



countless other roles. We are always seeking talent with experience in a variety of sectors, fields, or educational backgrounds. From security intelligence employees, IT professionals, service industry professionals or graduating students, rest assured, CSIS has a role for you.

In recent years, CSIS has made great strides in ensuring that its workforce is representative of Canadian society. Not only is this the fair and right objective, but it also ensures CSIS is operationally better as it can draw on the cultural, linguistic, and personal experiences of employees from across Canada. In support of ongoing efforts to foster diversity and inclusivity, we launched our Diversity, Equity, and Inclusion (DEI) Strategy in 2022 to provide a strategic framework for how CSIS intends to meet its objectives in this critical space. Ensuring a diverse workforce is critical to protecting national security, as having an in-house understanding of different cultures, practices, and beliefs are integral to building relationships with the countless Canadian communities we protect. The same can be said for the executive leadership at CSIS, which is why we strive to build a truly diverse executive team at CSIS to not only ensure significant decisions are informed by a variety of perspectives but also to ensure that CSIS better reflects the diversity of Canada and Canadians.

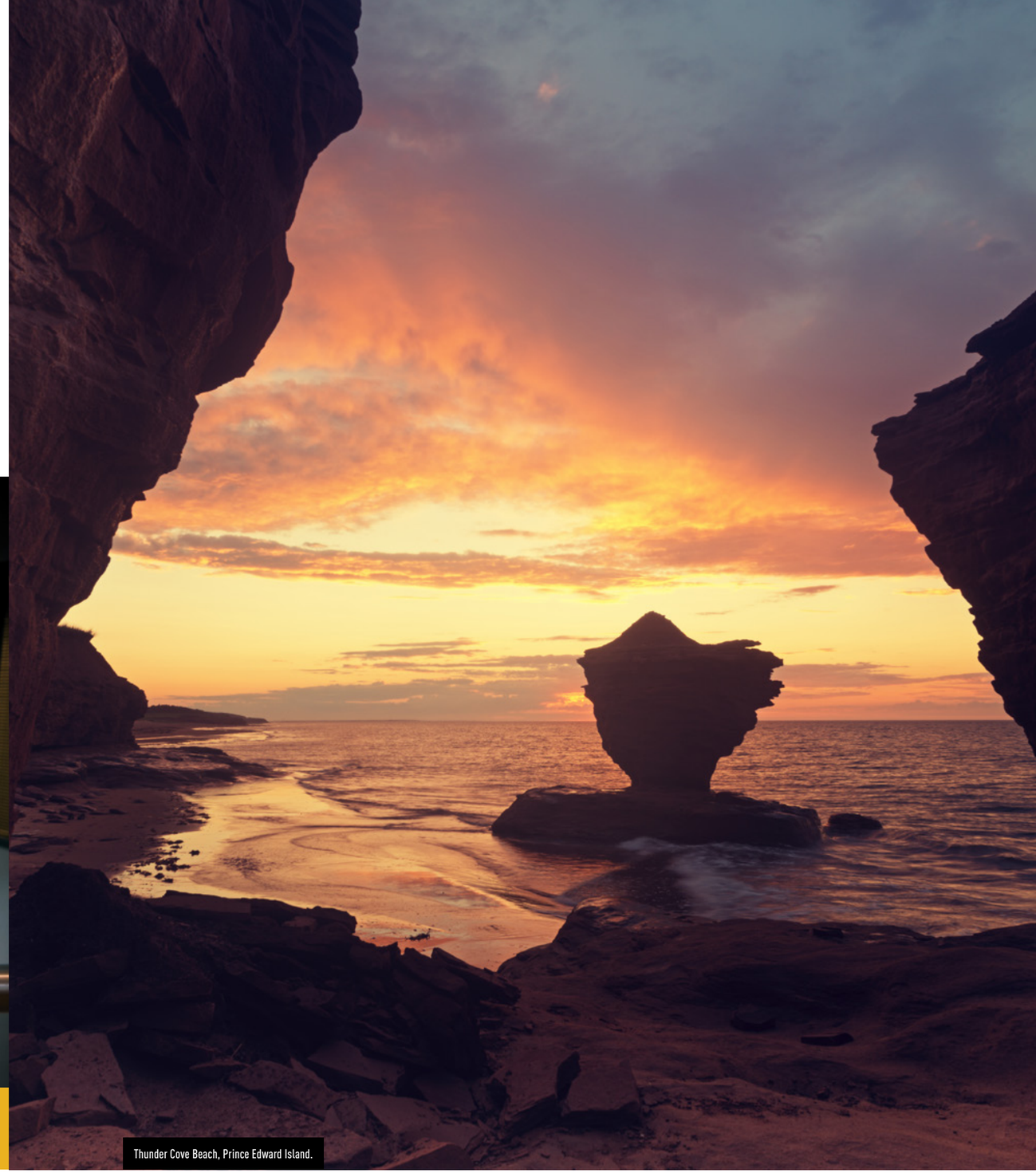
In pursuit of creating a workplace free of discrimination, bias, harassment, and aggression, we are taking action. In 2023, CSIS had 24 ongoing harassment investigations, and although some would use this metric to criticize CSIS, we believe it is indicative of the advancements we have made to improve our workplace culture, as more employees are now placing their faith and

confidence in CSIS' internal grievance process. In late 2023, we took further steps to bolster these processes when the Director committed to the establishment of an independent ombuds office during a December town hall address to all employees. The office will provide a trusted, confidential and impartial space for employees to openly discuss workplace-related issues or concerns. Culture change takes time, but I truly believe that we are making great strides towards the right path to becoming an organization that truly supports and respects all employees. Our employees and the citizens we serve deserve nothing less.

The people of CSIS truly make it a leading intelligence service. We are incredibly fortunate to be comprised of extraordinary and talented people who bring expertise, skill, dedication, and life experience, all of which is integral to ensuring CSIS is effective in successfully carrying out its mandate to protect all Canadians. As we continue on the path to transform CSIS into a more people-focused organization, we will continue to engage and hear the perspectives of our valued employees who give so much to undertake our mandate to serve and protect all Canadians. As Assistant Director of Human Resources of CSIS, it has truly been an honour and privilege of a lifetime to lead CSIS' workforce. ■

“The people of CSIS truly make it a leading intelligence service.”

Renée de Bellefeuille, Assistant Director of Human Resources at the Canadian Security Intelligence Service.



Thunder Cove Beach, Prince Edward Island.

Workplace Initiatives

In recent years, CSIS has made great strides in its effort to become a more people-focused organization that better supports all current and future CSIS employees.

Diversity, Equity, and Inclusion Strategy

In 2023, CSIS became the first Five Eyes intelligence service to publicly release its comprehensive Diversity, Equity, and Inclusion (DEI) Strategy.[5] Launched internally in 2022, the DEI Strategy lays out CSIS' commitments and actions for increasing diversity and inclusion in our workplace, while also advancing meaningful engagement with the diverse diaspora communities we protect. In 2023, CSIS has continued to make strides in advancing the Strategy and implementation of the three-year action plan. Implementation of the 45 commitments depends on a collaborative approach with multiple stakeholders across the organization. For transparency, CSIS tracks progress via a scorecard that is shared with all employees, as committed to in the action plan. In this regard, 78% of the commitments made in the action plan have progressed, and 20% of them are already completed.

CSIS 2023–2025 Accessibility Plan

In 2023, the roll out and implementation of CSIS' 2023–2025 Accessibility Plan[6] began as part of CSIS' efforts to make the organization more inclusive, accessible, and barrier-free. The multi-stakeholder plan requires various stakeholders across the organization to coordinate as they implement measures to make CSIS a barrier-free environment that supports diverse employees with disabilities.

CSIS has embraced the Government of Canada's guiding principle of "Nothing Without Us" in the development and implementation of CSIS' Accessibility Plan. The direct participation of CSIS employees with disabilities helps CSIS ensure that its accessibility initiatives are not just compliant, but genuinely responsive to the needs of all employees. During its inaugural year, 83 of the 102 activities committed to have advanced in some way, with 21 these activities reported as completed.

Noteworthy accomplishments

- Increased representation of diverse employees at CSIS.
- Launch of a more inclusive people management process.
- Integrating CSIS' commitment to DEI in the organizational strategic plan and consulting with CSIS' Diversity and Inclusion Advisory Committee about that plan.
- Regularly publishing comprehensive workforce dashboards to all employees detailing employment equity statistics and benchmarks.
- Issuing quarterly status updates to employees about DEI action plan progress.

Increasing Diverse Representation

In order to ensure CSIS' workforce is reflective of Canadian society and to serve communities better, recruitment is increasingly active in outreach and engagement efforts. The Diversity Recruiter role reaches out to and encourages diverse candidates to apply, and participates in career fairs, information sessions, and meetings as a part of efforts to increase diverse representation and meet CSIS objectives by 2026–2027.

Employee Engagement through Networks and Committees

CSIS values its employee-led networks, which bring employees together to have their unique perspectives heard. These networks include the Pride Network, Black, Indigenous and Persons of Colour (BIPOC) Network, Women in IT Plus, and the CSIS Women's Network. On September 15, 2023, CSIS employees also formalized and launched the Black Women's Network (BWN), which is active in supporting members and engaging with organizational leaders. This network is a platform for collaboration, empowerment, and fostering a stronger sense of community among Black women at CSIS. It is a space where they can celebrate achievements, support one another's growth, and drive positive change both

inside and outside the organization. All CSIS networks are a testament to the commitment of people across CSIS to fostering an inclusive workplace for everyone.

CSIS Cares – Government of Canada Workplace Charitable Campaign 2023

CSIS employees across Canada took part in the Government of Canada Workplace Charitable Campaign (GCWCC) in 2023, raising substantial funds while having fun and continuing to support our mission in the process.

CSIS kicked off GCWCC 2023 with an opening ceremony at National Headquarters (NHQ) in Ottawa. Employees from across Canada were able to tune in to the live-streamed event.

During the campaign, CSIS employees organized and participated in over 100 events and raised over $155,000 for charity.

- CSIS employees held over **100 events** across Canada.
- Over **100 volunteers** provided their time to facilitate events and collect donations for charities.
- Over **850 employees** participated in CSIS' annual sports day event.

Nahanni National Park Reserve, Northwest Territories.

Employee Demographics

	Representation (2022)	Representation (2023)	Objective by March 31, 2027
Persons with Disabilities	6.4%	7.1%	9.0%
Indigenous Peoples	2.2%	2%	3.4%
Racialized Groups	19.8%	20.7%	24.9%
Women in Science and Technology	17%	18.8%	24.9%

Executive Demographics

	Representation (2022)	Representation (2023)
Women	42.1%	42.3%
Indigenous Peoples	4.1%	3.8%
Racialized Groups	11%	14.1%
Persons with Disabilities	8.3%	9%

Expenditures

	2020–2021	2021–2022	2022–2023
Salaries*	$417,615,370	$404,107,049	$415,818,326
Operating	$259,284,331	$238,065,778	$256,628,550

*Salary costs include Employee Benefits Payments

Executive Spotlight – Deputy Director of Administration

Addressing the Unauthorized Disclosure of Intelligence

Jerome Laliberté, Deputy Director of Administration, Chief Financial Officer and Chief Transformation Officer, oversees the internal security program to protect CSIS, its employees, and assets.

In late 2022 and throughout 2023, classified CSIS and Government of Canada intelligence was distributed in an unauthorized manner and subsequently published for public consumption. The information was allegedly provided by an anonymous source with knowledge of national security affairs. Although some may praise the actions of the individual, unauthorized disclosure, no matter the motive or intent of those carrying out the act, causes significant harm to national security and the safety of Canadians.

Adversaries are consistently searching for new avenues to undermine Canada's security. Unauthorized disclosure of classified information can endanger intelligence collection methods used by CSIS. Much of the intelligence collection is about human interaction and human sources, who serve as important providers of the intelligence that is collected and analyzed by CSIS. Often, these sources are members of the general public who put their own safety at risk to offer valuable information in support of national security investigations.

There are times when a particular piece of intelligence can come from a single person or piece of technology. When this intelligence is exposed in an unauthorized manner, ill intentioned people and adversaries could trace the intelligence back to the source. Exposing these sources, even inadvertently through unauthorized disclosure, can threaten lives and national security investigations alike. In the wrong hands, adversaries can take advantage of the situation by implementing measures to reduce the effectiveness of CSIS' counter-intelligence and counter-terrorism operations, which can result in putting the lives of brave Canadians, working diligently to support the security of Canada, at risk.

The unauthorized disclosure of classified information reduces CSIS' ability to help protect our national interests, innovation, economy, and puts the personal safety of Canadians both domestically and abroad, at risk from threats posed by hostile state actors and violent extremist organizations. Moreover, it erodes the hard-earned trust of Canada's closest allies and intelligence partners, who may begin to doubt our ability to protect not only our own secrets, but theirs as well.

Jerome Laliberté, Deputy Director of Administration at the Canadian Security Intelligence Service.

In response to the unauthorized disclosures, CSIS launched an internal investigation and supported other investigations across the Government of Canada, including the RCMP's investigation into the matter. Current and former Government of Canada employees who obtained security clearances have a legal responsibility to protect classified information—a responsibility that extends beyond their employment with the federal government. There are legitimate reasons for this, and divulging classified information should not be treated as a noble act.

CSIS employees are dedicated and professional in carrying out their mission. Unauthorized dissemination undermines their efforts in painstakingly collecting and analyzing information on investigations. Unlawful sharing of intelligence poses a direct threat to Canada's national security.

There are processes in place within the Government of Canada that allow individuals to express concerns related to classified matters in a manner that does not damage Canada's national security and place the safety and security of human sources and national security employees at risk. It is paramount that these processes are followed. ■

Conclusion

Consult the CSIS Public Report online at www.canada.ca/CSIS

As Canada's security intelligence service, CSIS is committed to protecting Canada's national security, interests, economic prosperity, and people from threats both foreign and domestic. As CSIS enters its 40th year of protecting Canadians in 2024, CSIS will continue to grow, learn, and adapt to ensure it remains one step ahead of Canada's adversaries and threat actors who seek to undermine the security of our nation. In pursuit of this mission, CSIS will continue to engage with a broad range of national security partners to foster informed dialogue on national security matters, and increase collective resilience against threats to ensure the continued safety, security, and prosperity of Canada and all Canadians.

For more information, contact us at:

PO Box 9732 STN T
Ottawa ON K1G 4G4
Canada

Telephone: 613-993-9620
TTY and or TDD: 613-991-9228

Web Links

1. https://twitter.com/csiscanada/status/1671224330359799817
2. https://twitter.com/csiscanada/status/1726705344968327307
3. https://twitter.com/csiscanada/status/1740024893683417409
4. https://www.canada.ca/en/security-intelligence-service/corporate/publications/the-evolution-of-disinformation-a-deepfake-future.html
5. https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-diversity-equity-and-inclusion-strategy-2022.html
6. https://www.canada.ca/en/security-intelligence-service/corporate/accessibility.html