Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

CSIS Public Report

2022

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 2022*

www.canada.ca/CSIS

Published in March 2023

CSIS Public Report

2022

The Canadian Security Intelligence Service acknowledges that its 2022 Public Report was written and published on the traditional unceded territory of the Algonquin Anishinaabeg People.

Table of Contents

Highlights

Highlights

MISSION FOCUSED

Intelligence Reports

In 2022, CSIS produced over

2,500 intelligence products

Expanding CSIS Partnerships

Domestic Arrangements

87 arrangements with domestic partners

Foreign Arrangements

313 arrangements in **157** countries and territories

Immigration and Citizenship Screening Program

Requests received in 2022:

343,700

Government Screening Program

Referrals received in 2022:

149,620

Investment Canada Act (ICA)

CSIS screened

1,255

ICA notifications in 2021/2022 for national security concerns

Outreach

In 2022, CSIS conducted

113 stakeholder engagement activities

CSIS met with representatives of:

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

CSIS Briefings to Elected Officials in 2022

Federal **49** Provincial **26** Municipal **17**

PEOPLE FIRST

Executives who self-identified as a member of a racialized group has increased by 60% since 2019/20.

60% increase

Executives who self-identified as either a member of a racialized group, Indigenous Peoples and/or persons with disabilities increased from 14% in 2021 to 21% in 2022.

7% increase

ACCOUNTABLE TO CANADIANS

Access to Information and Privacy (ATIP)

***Privacy Act* requests** received in 2022

8% more *Privacy Act* requests than in 2021.

***Access to Information Act* (ATIA) requests** received in 2022

53% more ATIA requests than in 2021.

Informal requests received in 2022

49% more informal requests than in 2021.

For the 2022 calendar year, the **on-time compliance rates** stood at

95% for the *Privacy Act* requests

92% for the ATIA requests

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

	2021	2022
Ongoing reviews	17	18
Completed reviews	7	5

Social Media Analytics

@csiscanada

31% uptick in social media compared to 2021

Record Number of Parliamentary Appearances

225% increase compared to 2021

Message from the Director of CSIS

Message from the Director of CSIS

The year 2022 has been exceptional and transformative. If there is a lesson to take away from 2022, it is that very little is predictable. Major events can unfold in the blink of an eye, and now, more than ever, we must approach security threats with eyes wide open and in partnership. More than ever, Canada and Canadians depend upon their security and intelligence services to ensure they are safe, secure and prosperous. I am pleased to present CSIS's 2022 Public Report, which details how we have undertaken this vital mission.

We live in a time of intense global uncertainty where our national security is under constant threat; and that threat emanates from multiple vectors. The Russian Federation's unjustified and illegal invasion of Ukraine continues and foreign interference has intensified. These are but a few examples of the many attacks levied against the international rules based order, which are becoming all too frequent.

Here and around the world, the continued impact of the COVID-19 pandemic has reinforced the unpredictability of the current threat environment. It has exacerbated certain threats, and given rise to others. For example, we saw anti-public health measures protests grip our nation's capital and block border crossings in places such as Coutts and Windsor in early 2022.

Events like the Freedom Convoy protests revealed challenges across the security and intelligence community when dealing with a complex, multi-layered and dynamic situation that included both public order and national security components. Violent extremists of all motivations tend to exploit crisis situations and capitalize on fear, distrust, and uncertainty to spread their twisted worldviews, recruit others to their cause, and encourage acts of serious violence. Ideologically motivated violent extremism, or IMVE, is a complex threat comprised of a set of ideologies fuelled by extreme views around race, gender and authority. IMVE thrives on division, festers in the online space and radiates into other parts of society. The hateful rhetoric from these ideologies is becoming normalized and seeping into the mainstream. Canada has seen the real world impacts of antisemitism, Islamophobia and misogyny with devastating results. Approximately 50 percent of our counter terrorism resources are currently dedicated to investigating IMVE actors, influencers, and promoters.

The winter 2022 Freedom Convoy protests prompted a necessary and ongoing conversation about national security legislation in Canada, including the *CSIS Act*. This discussion featured renewed focus on the *CSIS Act* definition of threats to the security of Canada, enacted nearly 40 years ago. This definition has not always matched the expanding expectations from the Government and Canadians for information and intelligence from CSIS in the face of new and evolving threats.

While Canada continues to face violent extremist threats to our safety and security, foreign interference targets Canada's sovereignty, democratic institutions, prosperity and communities. We are seeing foreign states and their proxies target elected officials, communities, and the press in order to covertly influence Canadian policy, public opinion and our democratic institutions. To advance their economic interests, foreign states are undermining Canadian innovation and industry including by targeting our open academic and research entities.

We continue to see threat actors exploit social media to influence their intended targets. For example, state actors leverage it as a means to spread disinformation, divide public opinion and generally interfere in healthy public debate and discourse. Non-state actors, meanwhile, use it as a means to spread conspiracy theories and inspire violent extremist actions.

Canada has benefited from broad adherence to the rules-based international order, but it is clear that the world is evolving in a way that is not favourable to Canada as actors seek to exploit weakness within the rules-based system. However, it is also clear that CSIS is able to take action and respond to these threats by providing trusted intelligence and advice to help ensure a safe, secure and prosperous Canada.

CSIS will remain focused on its mission of protecting Canada and Canadians from all threats to our national security. It will recruit to enhance and retain its unique workforce and as an operational agency charged with protecting all Canadians, it will reflect the diversity of Canada. It will become a more digital and data-driven organization that capitalizes on technology while protecting the privacy of Canadians. And, as always, it will be accountable to Canadians.

It is often thought that the work of a security intelligence service occurs in the shadows, but I can tell you that we are committed to transparency with our country's citizens. It is essential for us to have the trust and confidence of Canadians to fulfill our mission. We will continue operating in a manner that is consistent with the democratic values that we hold dear and work hard to protect.

In 2022, we participated in a record number of Parliamentary committee appearances, enabling us to communicate openly with Parliament and all Canadians. We also participated in hearings related to the Public Order Emergency Commission, launched in response to the invocation of the *Emergencies Act*. CSIS employees are committed to transparency and, as Director, I will ensure that we continue to augment our work in this area.

Awareness is key to mitigate against foreign interference and espionage threats, and we are actively working to build resilience across Canada. To that end, CSIS has been delivering briefings to elected officials and their staff in all levels of government to better explain foreign interference and how it manifests. We are working with partners to help safeguard Canadian research and review investments that could present threats to national security.

I am happy to share that CSIS launched its employee-developed Diversity, Equity and Inclusion (DEI) strategy this past year. It is ambitious, but I believe that it needs to be; we are deeply committed to its implementation and to continuous learning. DEI, however, is not simply about representation in our workforce. For CSIS it is about meaningful engagement with diverse communities, to build and maintain trust and resilience to threats across our country. This engagement helps us to better understand the concerns of Canadians and inform our policies, programs and operations.

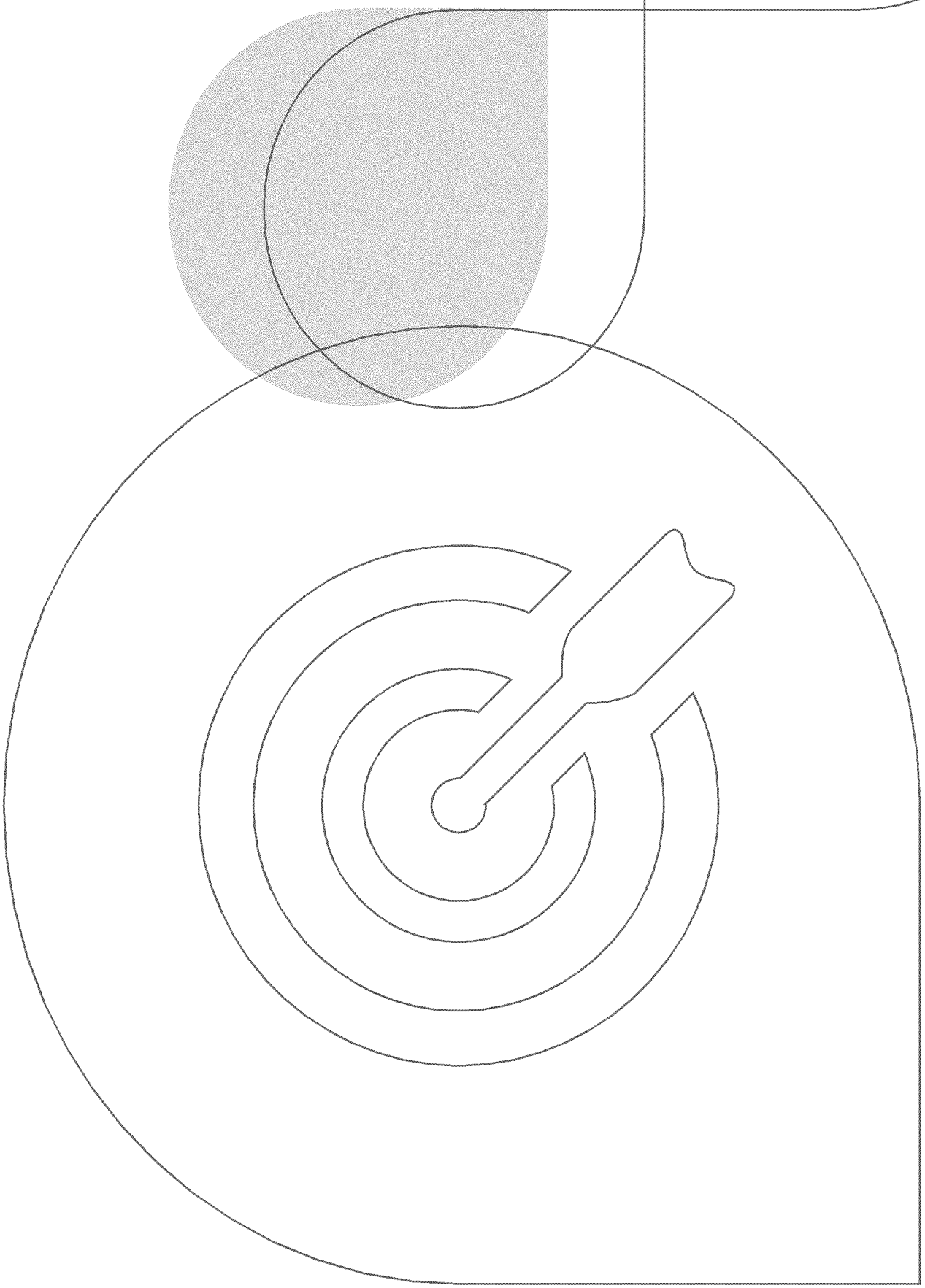
As Director, I am immensely proud of all CSIS employees and I am grateful to each of them for their personal commitment and dedication to the mission.

The threats to our country continue to accelerate. I am confident that the people of CSIS will work with our partners to tackle them head-on to keep Canadians safe, secure and prosperous, into 2023 and beyond.

Sincerely,

David Vigneault
Director of CSIS

“I am immensely proud of all CSIS employees and I am grateful to each of them for their personal commitment and dedication to the mission.”



Mission Focused: **Addressing the Threat Environment**

Duties and Functions

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

CSIS Responds

In an increasingly dangerous and polarized world, Canada faces multiple threats to our security, sovereignty, national interests, and values. CSIS is committed to keeping Canada and Canadians safe from all threats to our national security.

In doing so, 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 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.

In undertaking its work, CSIS reports on these threats by providing advice to the Government of Canada, including through the production of intelligence assessments and reports. In 2022, CSIS produced over 2,500 intelligence products. These assessments and reports are relied upon by Departments and Agencies to help inform policy making and to support evidence-based decisions. Separately, CSIS may also take measures to reduce threats to the security of Canada.

In addition, CSIS may collect foreign intelligence; that is, intelligence relating to the intentions, capabilities and activities of a foreign state. However, foreign intelligence may only be collected from within Canada at the request of the Minister of Foreign Affairs or the Minister of National Defence, and with the consent of the Minister of Public Safety.

CSIS also provides security assessments in support of Canada's ambitious immigration targets and to ensure the security of sensitive Government information, assets and sites. This security screening function and CSIS advice is vital to protecting Canada's national security.

All of CSIS's activities and operations must comply with Ministerial Direction and Canadian law, including the *CSIS Act* and the Charter of Rights and Freedoms.

The new, ever-evolving and persistent threat environment requires a nimble and dynamic operational approach. Canadians can be confident that when CSIS carries out its duties and functions, it acts in a manner consistent with fundamental Canadian rights and freedoms and in line with our democratic values.

Threat Reduction Measures in 2022

16 **Non-warranted TRMs**

CSIS was granted authority to undertake threat reduction measures (TRMs) under the *Anti-terrorism Act*, 2015. A TRM is an operational measure undertaken by CSIS, whose principal purpose is to reduce a threat to the security of Canada. CSIS identifies three broad categories of TRMs: messaging, leveraging, and interference. CSIS has not undertaken any warranted TRMs in 2022.

Foreign Interference

The *CSIS Act* defines foreign influenced activities as activities that are "detrimental to the interests of Canada and are clandestine or deceptive, or involve a threat to any person." These activities are also commonly referred to as 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 constitutes a threat to Canada's social cohesion, sovereignty, and national security.

To achieve their objectives, these foreign state actors engage in hostile activities such as clandestinely spreading misinformation and disinformation to undermine confidence in fundamental government institutions or electoral processes. They do so by cultivating witting or unwitting individuals to assist them, which enables them to operate with plausible deniability on Canadian soil.

In addition, foreign state actors monitor, intimidate and harass diaspora communities in Canada. They also attempt to silence dissidents and promote favourable narratives. Often, individuals fleeing repression or seeking a better life in Canada are discovering that sanctuary is hard to find. In a globalized world where no one is out of reach, states may exploit cyber capabilities to target individuals and institutions in Canada.

In 2022, it was reported that sub-national affiliates of the People's Republic of China (PRC) Ministry of Public Security (MPS) had set up three overseas "police stations" in Canada, without permission from the Government of Canada. CSIS has observed instances where representatives from various investigatory bodies in the PRC have come to Canada, often without notifying local law enforcement agencies, and used threats and intimidation in attempting to force "fugitive" Chinese-Canadians and Permanent Residents to return to the PRC.

Foreign interference directed at Canada's democratic institutions and processes, at all levels of government, can be an effective way for a foreign state to achieve its immediate, medium, and long term strategic objectives. Foreign states—again, directly and via proxies—may seek to influence electoral nomination processes, shape public discourse or influence policy positions of elected officials using covert tactics. The purpose is to advance issues or policies that favour the foreign state, or to quell dissent.

These threat actors must be held accountable for their clandestine activities. CSIS will continue to investigate, identify and reduce the threats that foreign interference pose to Canada's national interests and sovereignty, and will work closely with domestic and international partners in this effort to advise government. We will also continue to inform national security stakeholders and all Canadians about foreign interference to the fullest extent possible under the *CSIS Act*, in order to build our national resilience to this pernicious threat.

Espionage

Hostile intelligence services continue to target Canadians for intelligence collection and asset recruitment. In addition to traditional espionage operations, countries such as the PRC and the Russian Federation rely on non-traditional collectors to facilitate intangible technology transfer (ITT).

Non-traditional collectors

Individuals **without formal intelligence training** who have relevant subject matter expertise (i.e. scientists, business people)

Intangible technology transfer (ITT)

A pervasive, persistent, and often undetectable **method to facilitate the transfer of knowledge and technology** from Western countries, including Canada. ITT is ubiquitous in nature and difficult to detect, thereby posing a significant threat to Canada's economic and national security.

As a global leader in research and innovation, Canada is a prime target for the PRC's intangible technology transfer efforts. China targets research through legal, illegal and other unregulated means in order to augment its science and technology sector.

The PRC government and the Chinese Communist Party (CCP) have established policies and strategic plans to encourage Chinese citizens, the diaspora, foreign scientists, and entrepreneurs to contribute to the development of the PRC's science and technology sector. These policies and plans aim to exploit the collaborative, transparent, and open nature of Canada's research and innovation sector in order to serve the PRC's economic, intelligence, and military interests. To achieve this, the PRC utilises talent plans such as the Thousand Talents Plan, talent recruitment stations, and state-funded scholarship programs such as the China Scholarship Council.

Economic and Research Security

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 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.

Investigating and assessing the use of hostile economic activities by state actors is a priority for CSIS. In the context of COVID-19, advances in medical and health research have underscored the strategic importance of protecting the bio-health landscape (from early stage research and development (R&D) all the way through to patient administration) from threats like cyber attacks and espionage. The high value targets of these threats are data and intellectual property. State-sponsored threat actors will use fundamental research data, personally identifiable health data and aggregate pools of medical and health data to advance their own biotechnology, intelligence and military objectives. In addition to protecting Canadian data, the bio-health landscape will also need to develop and maintain reliable supply chains for basic medical supplies, equipment, therapeutics and pharmaceuticals.

In 2022, CSIS continued to support Canada's research, health, and supply chain sectors' pandemic related efforts. To help protect Canadian innovation, intellectual property, and the valuable data that support them, CSIS provided dozens of briefings in academic forums. These briefings were delivered to individual universities and to research institutions, in support of the wider Government of Canada effort, led by Innovation, Science and Economic Development Canada (ISED). In 2022, CSIS also screened 1,255 ICA notifications for national security concerns.

CSIS is proud to contribute to the Government of Canada's agenda on research security, and will continue to provide national security intelligence and advice to help secure Canadian intellectual property and innovation. CSIS engaged a number of associations and companies in the emerging and deep technology sectors. The aim of CSIS's engagement was 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 access to leading edge and trusted technology. This vibrant and growing sector has ongoing research in areas as diverse as agri-tech, smart cities, and clean-tech.

In 2021, the Government of Canada published the *National Security Guidelines for Research Partnerships* to better position researchers, research organizations, and Government funders to undertake consistent, risk-targeted due diligence of potential risks to research security. Under these *Guidelines*, which are currently being phased in, CSIS is working closely with the Natural Sciences and Engineering Research Council of Canada (NSERC), Innovation, Science, and Economic Development Canada (ISED), Public Safety Canada, and other national security partners to assess certain applications for federally-funded research partnership grants for national security threats, as part of a risk assessment. These efforts aim to protect Canada's research ecosystem from foreign interference, espionage, and unwanted knowledge transfer that could pose a threat to Canada and against Canada's national security interests.

Cyber Threats

Canada remains a target for cyber-enabled espionage, sabotage, and foreign influenced activities that pose significant threats to its national security and advance the interests of hostile actors. In 2022, malicious cyber activity continued to increase in scale and complexity, illustrating the need for a high level of cooperation throughout the whole of government and with private industry.

Cyber threat actors include state-sponsored actors operating at the behest of nation-state intelligence services. They also include non-state actors, whose activities such as ransomware attacks on critical infrastructure, pose threats to the security of Canada, due in part to the disruptive impacts that they cause.

PRC state cyber actors continue to target a wide range of key sectors in Canada, including governments, academic institutions, defence contractors and civil society organizations. For example, there are multiple open source reports of PRC actors stealing the intellectual property and research data of targets, as well as stealing user account credentials and customer data to enable future cyberattacks.

Russian cyber actors continue to pose a significant threat to Canada. In April 2022, Canada and its allies issued a joint cyber security advisory warning that Russia's invasion of Ukraine could expose organizations in the immediate region—and beyond—to increased malicious cyber activity. In May 2022, Canada issued a statement condemning the destructive cyber activity by Russia targeting the European telecommunications sector on February 24, 2022, and joined its partners and allies in attributing this activity to Russia.

Certain types of cybercriminal activity are considered national security threats because of their impact. State actors increasingly use and benefit from cybercrime tactics that advance their objectives. Critical infrastructure will continue to be at high risk from these activities, as entities within these sectors continue to be perceived as having deep pockets and, therefore, more likely to pay as a result of their requirement to provide uninterrupted service.

A few hostile states such as Iran are expanding their cognitive warfare capability. These actors are integrating cyber operations and technologies with psychological operations to enhance their ability to influence targeted individuals and societies. The objective of cognitive warfare operations is to alter the worldview of the target group.

Foreign states that lack sophisticated cyber capabilities can now purchase increasingly available tools and services from commercial providers. Foreign governments with abysmal human rights records are leveraging these commercial software applications, to monitor dissidents, activists, journalists and community groups.

Violent Extremism

Violent extremism, whether it is religiously, politically or ideologically motivated, continues to represent a significant threat to public safety. The persistent threats of extremist violence and terrorist violence must be taken seriously. It is important to understand that extremism can stem from a range of motivations and personal grievances, driven by hatred and fear, and includes a complex range of threat actors.

Extremists draw inspiration from a variety of sources including books, music, and of course, online discussions, videos and propaganda. Those holding extremist views often attempt to create a culture of fear, hatred and mistrust by leveraging an online audience in an attempt to legitimize their beliefs and move from the fringes of society to the mainstream.

While only a small number of Canadians are actually willing to engage in serious violence in support of their extremist views, the impact of their actions can be devastating. Canada is not immune to acts of violent extremism.

Ideologically Motivated Violent Extremism (IMVE)

Ideologically Motivated Violent Extremism poses a significant national security threat and is on par with the religiously motivated violent extremism (RMVE) threat in Canada. A range of grievances motivate IMVE extremists' willingness to incite, enable, and/or mobilize to violence. These ideologies can be xenophobic and linked to neo-Nazism; anti-authority; identity and gender-driven; or based on other grievances without clear affiliation or external guidance.

Traditional IMVE groups with more structured leadership and defined objectives have been largely—although not completely—replaced by loosely networked, transnational movements with vague goals that co-exist across the IMVE milieu.

The COVID-19 pandemic exacerbated xenophobic and anti-authority narratives, many of which may directly or indirectly impact national security considerations. Violent extremists continue to exploit the pandemic by amplifying false information about government measures, the COVID-19 vaccine and the virus itself on the internet. These narratives have contributed to efforts to undermine trust in the integrity of government and confidence in scientific expertise. Some violent extremists view COVID-19 as a real but welcome crisis that could hasten the collapse of Western society (known as accelerationism).

IMVE threat actors often target equity-deserving groups including racialized individuals, religious minorities, the 2SLGBTQI+ community and women. In addition, CSIS has observed a marked increase in violent threats directed towards elected officials, government representatives and journalists. As a result of the accelerating IMVE threat environment, CSIS now dedicates 50% of its counter terrorism resources to investigating this threat.

Religiously Motivated Violent Extremism (RMVE)

Religiously Motivated Violent Extremism (RMVE) remains an investigative priority for CSIS and a threat to Canadian national security. CSIS will continue to work with community stakeholders in order to address it in partnership. Canadians and Canadian interests abroad have been and continue to be the targets of RMVE acts in an ever-evolving global threat landscape.

The ongoing RMVE threat in Canada comes primarily from individuals or small groups informally aligned to, or inspired by, DAESH and Al Qaeda (AQ). Their ideologies can be fluid and the threat increasingly originates from youth, primarily online. There is a propensity to mobilize to violence quickly, using low-tech means to take action against soft targets.

In 2022, DAESH was under pressure on multiple fronts but it still seeks to re-establish a Caliphate by continuing to conduct insurgent attacks. DAESH affiliates have also demonstrated increased activities, expansion and operational reach, particularly in Sub-Saharan Africa.

Canadians who work or travel near the Horn of Africa and West Africa continue to face significant threats such as kidnap-for-ransom operations by Al Qaeda-aligned Al-Shabaab (AS) and Jamaat Nusrat al-Islam Wal Muslimin (JNIM).

Counter-Proliferation

The proliferation of chemical, biological, radiological and nuclear (CBRN) 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. For example, Iranian-made Shahed-136 drones used by Russia against Ukrainian civilians consist almost entirely of foreign-made parts, including Canadian technology.

CSIS continues to work closely with domestic and foreign partners to uphold the Government of Canada's commitment to counter-proliferation. This entails efforts to detect, investigate, prevent and disrupt activities in or through Canada involving the illicit acquisition, export or diversion of goods that may enable WMD programs. These efforts also extend to intangible technology transfers.

CSIS continues to provide ongoing support to a range of Government of Canada sanctions and related measures against a number of countries, including Russia and Iran, under the *Special Economic Measures Act* (SEMA) and the *Justice for Victims of Corrupt Foreign Officials Act* (JVCFOA). These sanctions include asset freezes and the prohibition of certain activities—for example, financial assets, property, and trade in certain technologies and dual-use goods subject to export control—with designated persons and entities of the sanctioned countries. Furthermore, as senior officials of the Iranian regime are now inadmissible under the *Immigration and Refugee Protection Act* (IRPA), CSIS works closely with its immigration partners to enforce this designation.

Security Screening

Immigration programs enable the Government of Canada's economic, prosperity and post-COVID recovery agenda. Immigration accounts for a big part of labour force growth in Canada, including specific labour market needs. It also builds a more diverse Canada, which is a stronger Canada. Through its Government Security Screening (GSS), and Immigration and Citizenship Screening (ICS) programs, CSIS serves as the first line of defence against violent extremism, espionage, and other threats to national security by preventing exploitation by a small number of nefarious actors.

The GSS program conducts investigations and provides security assessments to departments and agencies in order to prevent individuals of security concern from gaining access to classified or sensitive information, assets, sites and major events. Security assessments are part of an overall evaluation to assist federal government departments and agencies in deciding to grant, deny, or revoke security clearances based on national security concerns. These decisions rest with each department or agency, and not with CSIS. Additionally, CSIS plays a key role in ensuring that sensitive Canadian information, research and data is properly protected, for the benefit of all Canadians.

GSS also conducts screening to protect sensitive sites—including airports, marine, and nuclear facilities—from national security threats. Furthermore, it assists the RCMP in vetting Canadians and foreign nationals who seek to participate in major events in Canada. Finally, GSS provides security assessments to provincial and foreign governments, and international organizations, when Canadians seek employment requiring access to sensitive information or sites in another country. In 2022, CSIS received 149,620 requests for GSS.

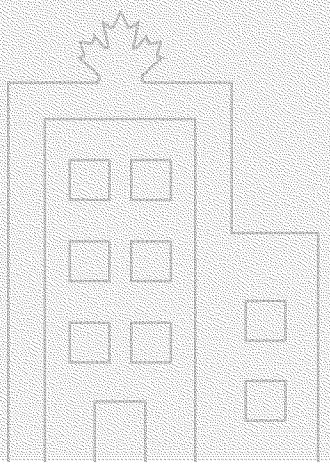
The CSIS ICS program provides security advice to the Canada Border Services Agency (CBSA) and Immigration, Refugees and Citizenship Canada (IRCC) regarding persons who may represent a threat to national security and are attempting to obtain entry to or status in Canada. IRCC officers assess applications, and if admissibility concerns are flagged, the application may be referred to CBSA and CSIS for comprehensive security screening. Through this risk-based program, CSIS provides security advice on permanent resident and citizenship applicants; persons applying for temporary resident visas; and persons applying for refugee status in Canada. CSIS received 343,700 referrals in 2022.

As part of this, CSIS continues to screen applicants from Afghanistan, referred by IRCC, as part of the Government of Canada's commitment to resettle at least 40,000 Afghan refugees by the end of 2023. The completion of inadmissibility screening is a regular part of the review process for resettlement applications.

Following Russia's full-scale invasion of Ukraine in February of 2022, the Government of Canada committed to providing safe haven to Ukrainians and their families fleeing Russian aggression. By late December 2022, Canada had received over 755,000 Temporary Residency Visa applications under the Canada-Ukraine Authorization for Emergency Travel (CUAET) and had welcomed over 100,000 Ukrainian citizens. Timely security advice was critical in making this happen. CSIS will remain ready to assist as long as Russian aggression continues and civilian populations face displacement.

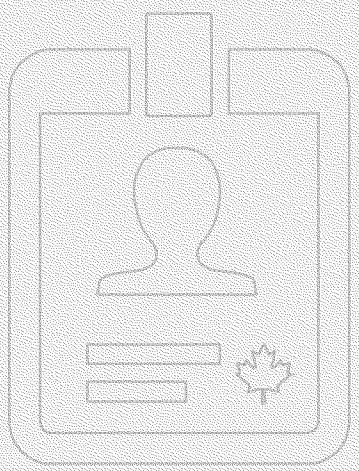
Immigration and Citizenship Screening Programs

2022	REFERRALS RECEIVED*
15,300	Permanent Residents Inside and Outside Canada
55,500	Refugees (Front-End Screening**)
252,500	Citizenship
20,400	Temporary Residents
343,700	**TOTAL**



Government Screening Programs

2022	REQUESTS RECEIVED*
56,100	Federal Government Departments
8,600	Free and Secure Trade (FAST)
63,500	Transport Canada (Marine and Airport)
2,900	Parliamentary Precinct
11,700	Nuclear Facilities
120	Provinces
2,200	Others
500	Foreign Screening
4,000	Special Events Accreditation
149,620	**TOTAL**



*Figures have been rounded

**Individuals claiming refugee status in Canada or at ports of entry (i.e. asylum claims)

Threat Challenges Ahead

Increasingly Polarized World and Ideologically Motivated Violent Extremism

In 2022, Canadians were exposed to more sophisticated conspiracy theories and alternative information. Doctored evidence and manipulated audio and visual files such as deep fakes have become commonplace.

Conspiracy theories:

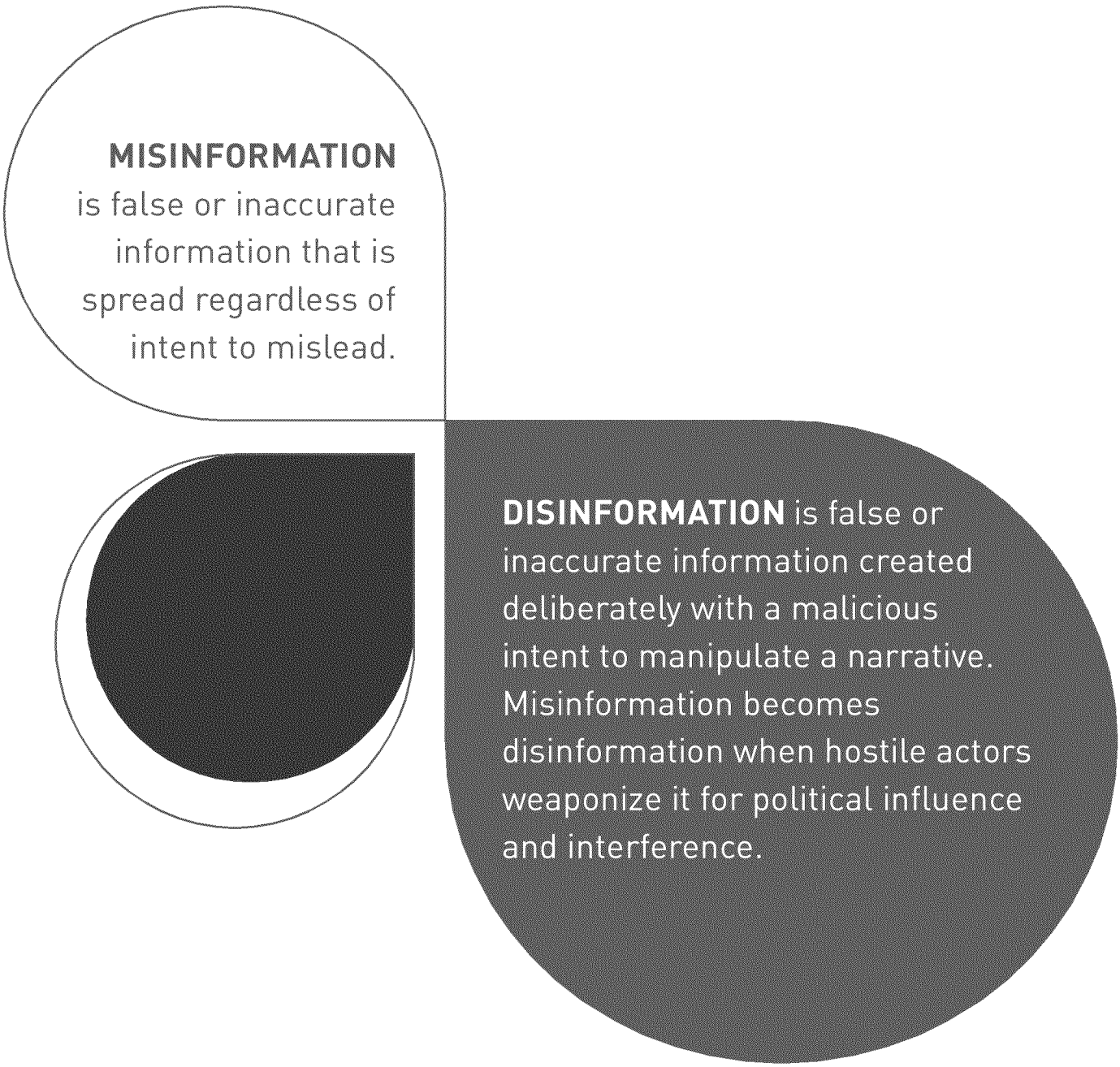
- Demonize out-groups
- Victimize in-groups
- Delegitimize dissent
- Counter official/established narratives
- Encourage individuals to turn to violence for 'self-defence'

IMVE actors who have mobilized to violence commonly cite conspiracies, combined with personal grievances and ongoing national debates, as a source of motivation. The rapid spread of IMVE narratives online adds to the national security challenge.

The 'weaponization' of conspiracy theories continues to be widespread in the IMVE milieu. The emergence of Canadian "influencers" who have gained significant followings have done so through their promotion of conspiracy theories and have been enabled to push their messaging via a variety of social media platforms, encrypted messenger applications, and foreign state-affiliated media. While much of today's IMVE activity occurs in the online sphere, the Canadian landscape reveals an increase in face-to-face activity, which will most likely increase post-pandemic.

Misinformation / Disinformation

CSIS observed the continued spread of misinformation and disinformation by state and non-state actors in 2022. Threat actors are aware of the impact the proliferation of information manipulation has on open democratic societies, and continue to target Canadians. As more Canadians transition from conventional media to a digital news environment, malicious state actors have exploited this transition via proxy amplifiers on social media to support their messaging. Users' ability to engage with content through "likes" and "shares" adds to social media's potency to boost disinformation and impact audiences that would otherwise be beyond reach. Social media's ability to bring fringe views into the mainstream public discourse enables state actors to polarize Canadian public opinion through repeated exposure to conspiratorial messaging. Online platforms can serve as echo chambers of hate where like-minded individuals are able to connect and communicate anonymously and mobilization to violence can occur rapidly.



The Indo-Pacific

The People's Republic of China (PRC) has unresolved territorial disputes in several areas on its periphery. In parallel with the PRC's growing economic and military power, People's Liberation Army (PLA) units and government entities have been seeking to solidify territorial claims. They do so by using a strategy of taking a series of measures that are below the threshold of armed conflict and small enough to avoid provoking a violent response. However, these measures cumulatively create difficult-to-reverse "facts on the ground", serving to alter the status quo and normalize a situation where PRC claims are strengthened and related interests are advanced.

On November 27, 2022, the federal government publicly announced Canada's new Indo-Pacific Strategy (IPS). The IPS is a clear-eyed approach to the risks and opportunities of the region, and its strategic importance. It serves both to reap its potential economic rewards, and to meet the national security challenges in the region. This is a landmark strategy with significant implications for our country, and CSIS will play a key role in supporting its implementation.

Under the IPS, CSIS will make critical investments and improve capabilities to help protect the safety, security and prosperity of Canada and Canadian interests. CSIS will work alongside its security and intelligence partners to deliver on the IPS. CSIS's objectives include:

1. **Grow CSIS's partnerships and engagements with the region.**
2. **Increase capacity to counter threats and hostile activities emanating from the region.**
3. **Counter domestic threats resulting from increased engagement with the region, such as informing Canadian stakeholders of risks relevant to their increased involvement in the region.**

Ukraine – Protracted Conflict

The year 2022 saw growing challenges to the rules-based and open international order. These challenges came from shifting centres of global influence and from actors willing to exploit uncertainty to advance their own interests, culminating in an explosive and potentially devastating blow to the global security framework. The Russian Federation's illegal invasion of Ukraine in February 2022 has directly threatened world security, while also affording Russia and its supporters worldwide an opportunity to step up their disinformation-based propaganda campaigns in the West, including in Canada. Sharply exaggerated narratives aim to discredit Ukraine and undermine public support for the continuing military aid to Ukraine. These narratives are targeting both Russian and Ukrainian communities in Canada with misinformation and disinformation through increasingly powerful social media platforms.

Arctic and Northern Canada

The Arctic must be protected as an important part of Canada's sovereignty and in the interest of North American continental and maritime security. For a number of reasons, the economic and strategic importance of the Arctic has been steadily growing over the past 15 years. Along with growing commercial and international interests,

the variety of threats to Canada's security and sovereignty has also grown. In this context, security threats to the Arctic do not come only in conventional military form or from climate change, but also in the form of espionage, foreign interference (FI) activities and economic initiatives, which all can represent national security threats to Canada. CSIS is proud to work with Inuit partners and lend our support to the Government's overall strategy to ensure safety and security in the region.

Afghanistan

The Taliban faces significant challenges governing Afghanistan, which is in an economic and humanitarian crisis that will likely continue to 2023 and beyond. The Taliban has implemented statewide repression, denying human rights to women and religious and ethnic minorities with the objective of creating a 'pure' Islamic system.

The Taliban has continued to allow transnational terrorist groups, such as Al Qaeda (AQ) to remain in the country. While AQ activities in Afghanistan remain limited, there is a possibility that it will once again view Afghanistan as a safe training ground.

Notwithstanding some degree of opposition by the Taliban, the Islamic State Khorasan Province (ISKP) has had the opportunity in 2022 to position itself as a local, regional, and possibly international threat. ISKP could gain momentum in 2023 by regaining basing areas in eastern Afghanistan, thereby entrenching itself in a manner previously prevented by the presence of international forces.

Russian Private Military Contractor – Wagner

Anti-Western sentiment in Mali, Burkina Faso and Niger has increased notably. France withdrew its military force from Mali in 2022 and from Burkina Faso in February 2023. The influence of Russian private military contractor (PMC) Wagner in Mali and Burkina Fasi has increased, and Wagner continues to expand Russian influence and undermine Western interests.

Wagner is likely applying known strategies such the use of disinformation campaigns to target any perceived rivals or Western interference. CSIS assesses that Wagner will continue to leverage the security void and the reduced participation of Western countries in the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA).

Security Implications of Returning Canadian Extremist Travellers (CETs)

Almost a decade after their initial mobilization, DAESH affiliated Canadian Extremist Travellers are returning to Canada from camps in Syria and Iraq. Although CET returnees may not immediately or directly engage in extremist violence, they still pose a national security risk. They have been exposed to radical influences, violence, repression and many have received weapons and explosives training. In time, CETs may engage in extremist activities such as fundraising, maintenance of domestic and international networks, radicalization and/or recruitment. CSIS is committed to working closely with its domestic and international partners to protect Canadians against threats to our security from returning CETs.

Engaging with Canadians

CSIS continues to seek out opportunities to engage directly with Canadians on issues of national security to build awareness, trust and resilience to threats. CSIS is proud of its strong relationships with Canadian communities that have developed over many years and are based on mutual trust and respect. This is in addition to the 92 briefings of elected officials at all levels of Government that CSIS provided in 2022.

CSIS Briefings to Elected Officials in 2022

Federal 49 **Provincial** 26 **Municipal** 17

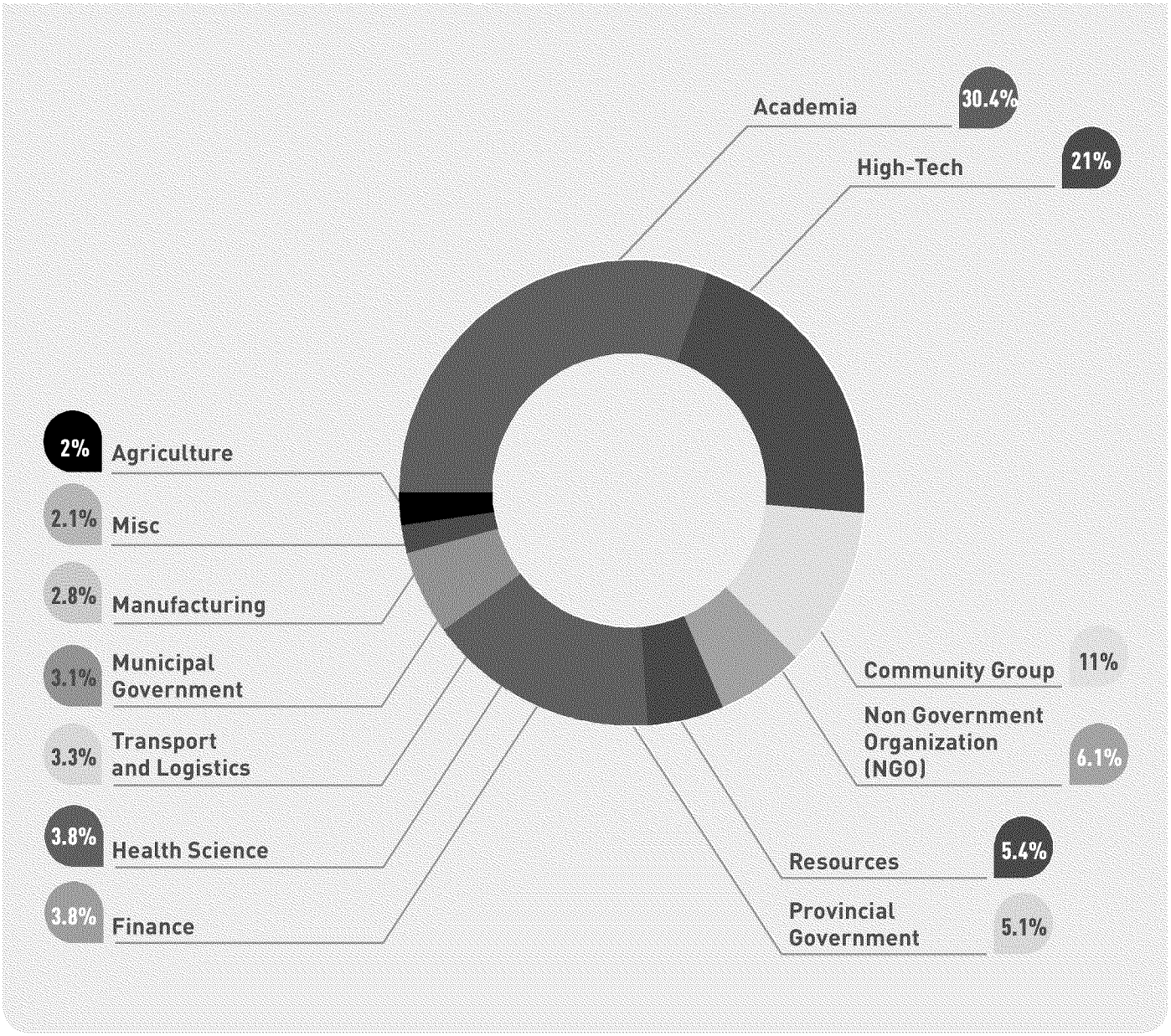
Outreach in 2022

One focus of engagement in 2022 was on building relationships with communities to help ensure they have the information and support needed to deal with threat related activities, particularly involving foreign interference and extremism. CSIS shared information and resources with members of Asian Canadian communities in Canada to raise awareness about foreign interference activities in Canada, including those targeting diaspora communities. CSIS also released a new guidance document in 2022 focused on a whole-of-society approach to combatting extremism entitled, *Protecting National Security in Partnership with All Canadians*[1]. This document is available on CSIS's website and is currently being translated into additional languages to ensure wide accessibility. In 2022, CSIS also issued a public report entitled Foreign Interference and You[2] to increase awareness and build resilience among Canadians on this important threat to the security of our country. This was published in six languages, so that as many Canadians as possible can be reached. In addition, CSIS increased engagement with Indigenous communities.

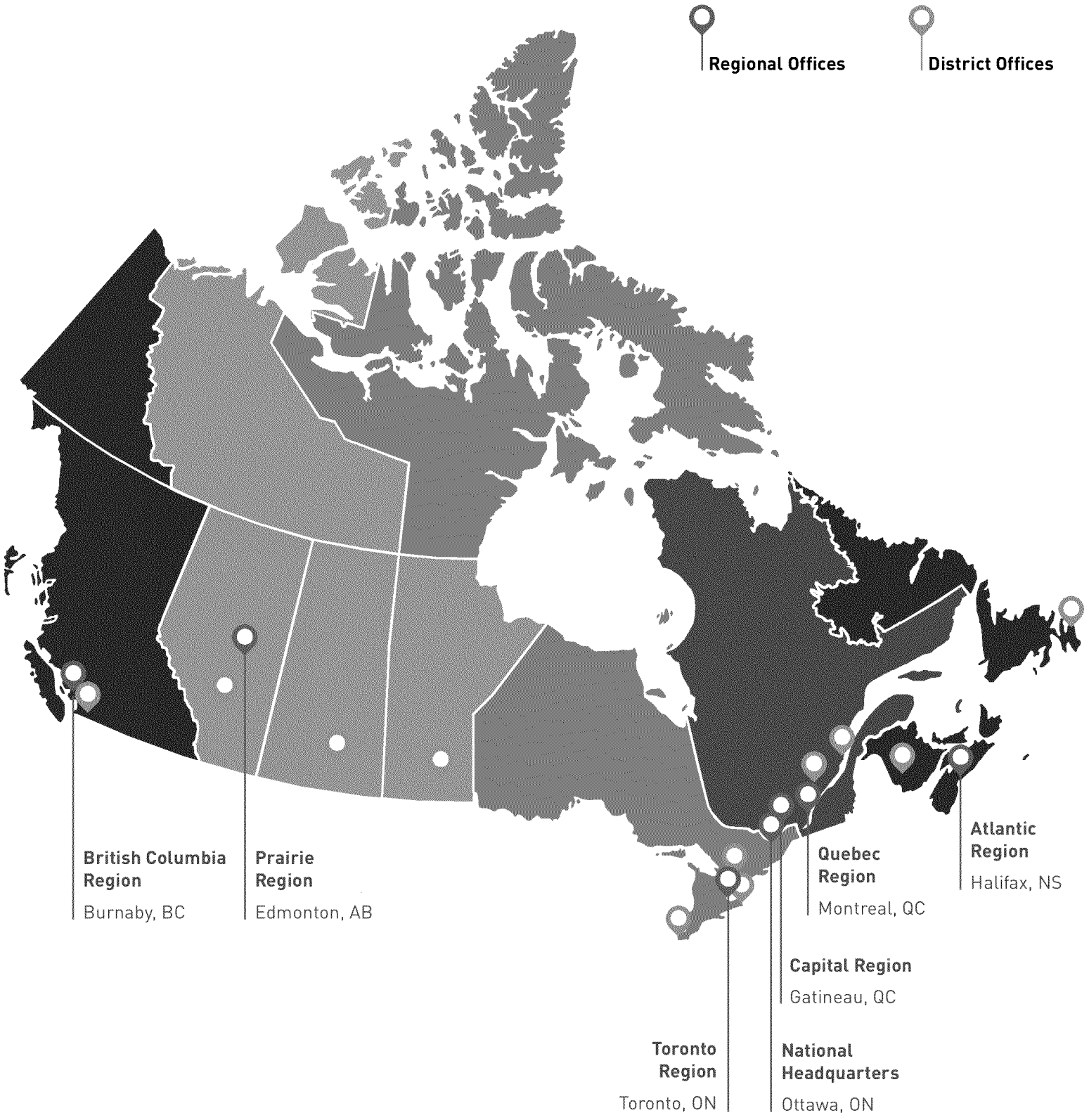
In 2022, CSIS hosted 14 virtual expert briefings, produced 14 commissioned reports, facilitated two expert roundtables, and provided feedback from a national security lens on two Government of Canada funding advisory boards. In addition to mobilizing knowledge from a wide variety of academic experts, CSIS also continued to mentor university students including a cohort of graduate-level students at the School of Public Policy and Global Affairs at the University of British Columbia. CSIS officials also participated in class and seminar discussions at universities across Canada to support healthy debate with students on national security-related issues.

In 2022, CSIS conducted 113 stakeholder engagement activities and met with representatives of academia; community organizations; civil society and advocacy associations; research and innovation institutes; Indigenous leaders; as well as representatives of provincial and municipal governments. Now more than ever, national security is not the exclusive remit of the Government of Canada. As it continues to engage stakeholders in dialogue on national security matters, the limits on CSIS's ability to share classified information and advice are having an impact.

Summary of Engagements by Sector



CSIS across Canada



Advancing Truth and Reconciliation

CSIS's evolving work in developing relationships with Indigenous partners is part of its commitment to the Truth and Reconciliation Commission's recommendations. As part of its priority engagement with Indigenous partners in 2022, senior-level CSIS delegations travelled to Inuit Nunangat to establish relationships with local and regional organizations. These meetings represented unique opportunities for CSIS to learn first-hand about the culture and traditional livelihood of Inuit, and most importantly, to lay the foundations for long term relationships between Inuit and CSIS. Territorial stakeholders were also engaged during these visits, allowing CSIS to further strengthen existing operational relationships.

CSIS raised internal awareness of Missing and Murdered Indigenous Women and Girls, Indigenous history and cultures. To enable land acknowledgements wherever employees meet or gather, CSIS encourages employees to make land acknowledgements in all of its offices. An Indigenous Elder visited CSIS to bless the Orange Flag when it was hoisted to recognize National Day for Truth and Reconciliation.

Integrated Terrorism Assessment Centre (ITAC) Profile

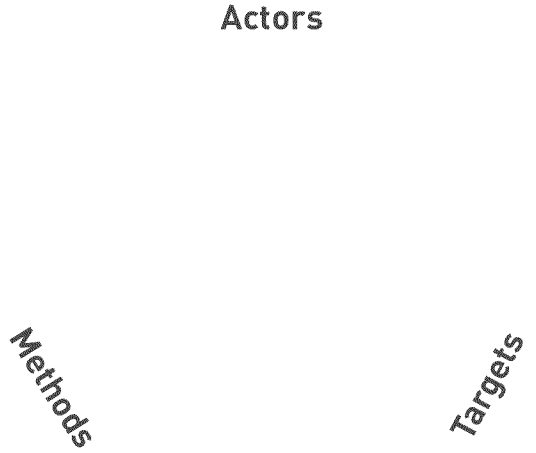
The Integrated Terrorism Assessment Centre (ITAC), created in 2004, was established to independently produce comprehensive threat assessments using a wide range of classified and unclassified sources. ITAC serves as a "community resource" to support government decision-making and provide timely analyses to security partners.

ITAC is co-located within the Canadian Security Intelligence Service's (CSIS) headquarters and operates under the provisions and authorities of the *CSIS Act*. The Centre does not collect intelligence, and instead relies on intelligence collected by domestic and international partners, including CSIS, and openly available information, to produce its assessments.

Specifically, ITAC has three main program areas:

- Assessing and reporting on terrorism threats, trends and events;
- Assessing and recommending the National Terrorism Threat Level (NTTL) for Canada;
- Assessing and setting terrorism threat levels for Canadian interests worldwide, including for special events.

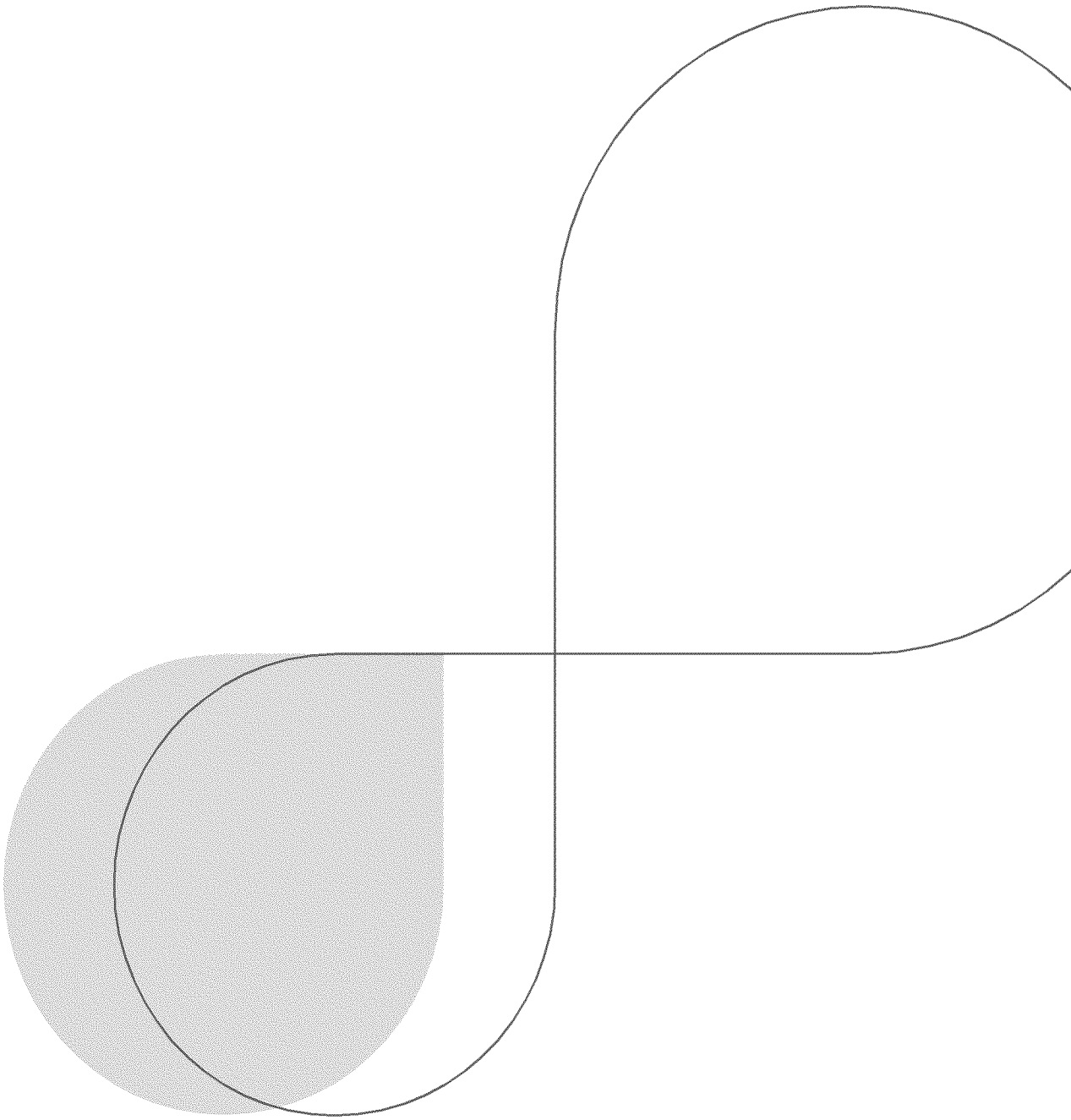
ITAC's threat assessments are based on a rigorous methodology that analyzes quantitative and qualitative indicators pertaining to the intent, capability and opportunity of potential threat actors to conduct an act of terrorism. These assessments serve several functions, including raising awareness of the threat environment and informing security mitigation measures.

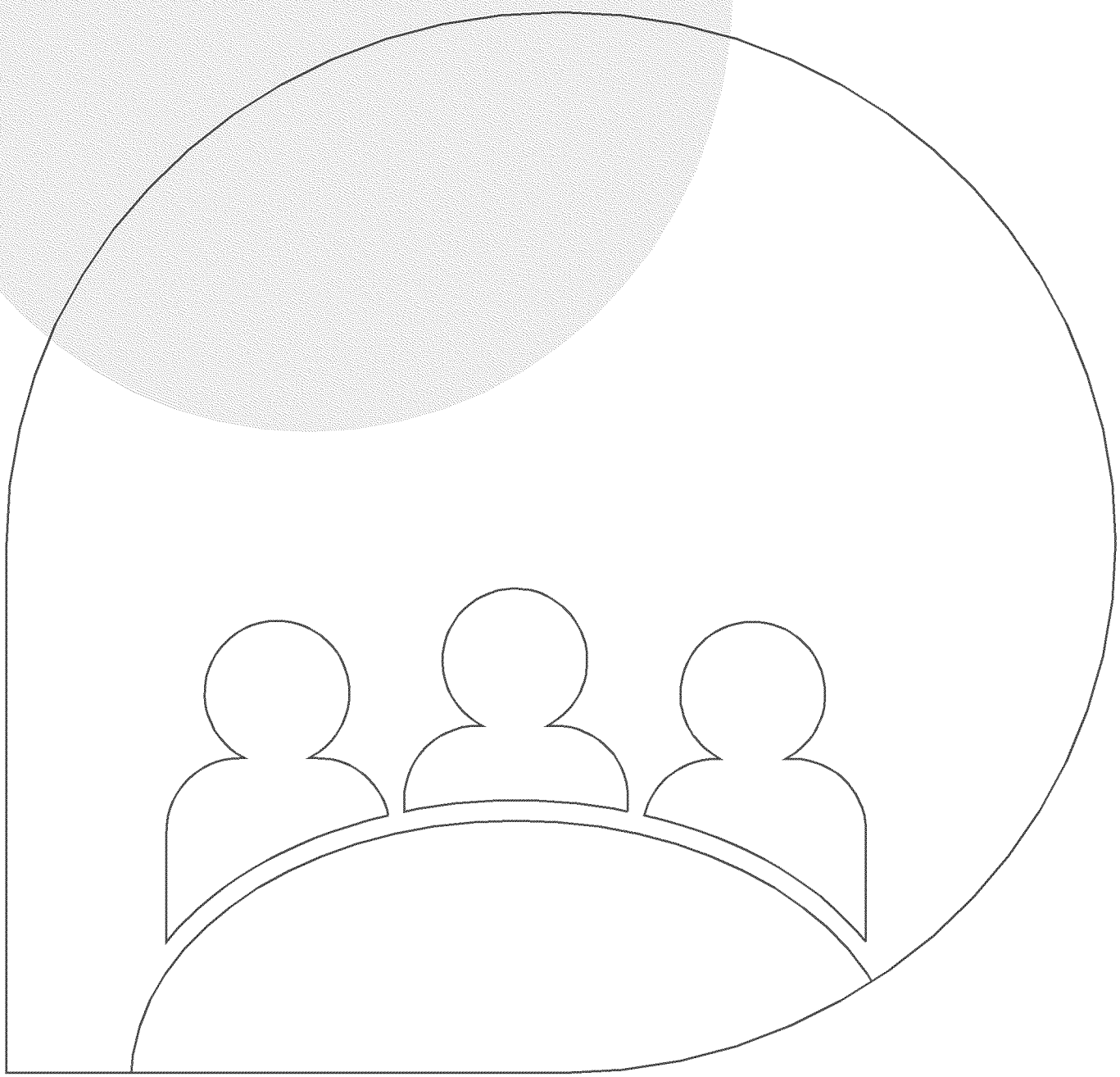


ITAC has a very broad dissemination mandate. Beyond senior government officials and federal security partners, it disseminates reports to provincial, territorial and municipal law enforcement agencies, as well as to critical infrastructure stakeholders.

The National Terrorism Threat Level (NTTL)

The NTTL, which is reassessed at least every four months, provides a common understanding of the general terrorism threat facing the country. It represents the likelihood of a violent act of terrorism occurring in Canada. The comprehensive analysis that supports the NTTL provides detailed insights on the evolving threat landscape, and on where and how particular threats could materialize.



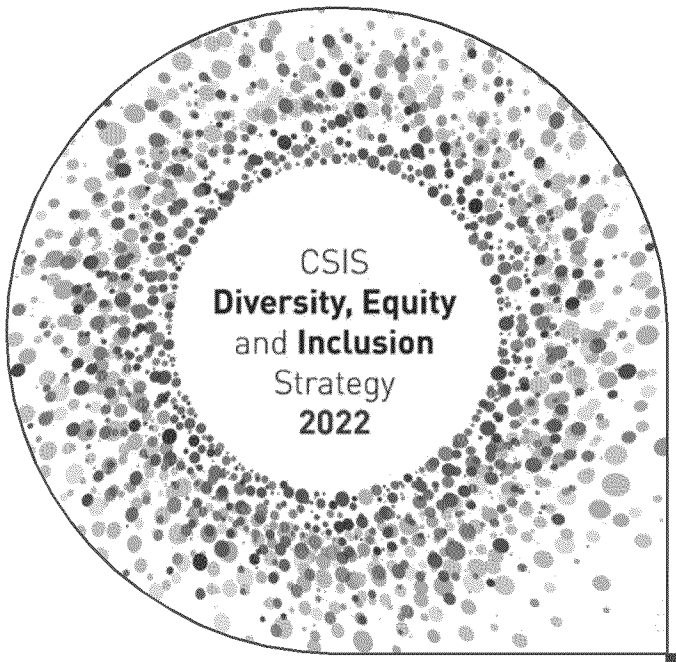


2

People First: **Investing in our Workforce to Deliver our Mandate**

Diversity, Equity and Inclusion

To fulfill its mission, CSIS must recruit, develop and retain highly skilled and diverse employees who work together to protect Canada and Canadians. CSIS is committed to building a workforce that is truly representative of the Canadians it serves by cultivating a diverse and inclusive workplace environment. Our commitment to diversity and inclusion is a key pillar in our ability to succeed in our mission. Our diversity allows us to better understand all the Canadian communities we protect. Increasing employment equity group representation—including persons with disabilities, visible minorities, Indigenous peoples and women—at all levels within the organization through hiring and talent management practices is a priority. CSIS continues to attract and retain a top performing and diverse workforce.



A Diversity, Equity and Inclusion (DEI) Strategy of which to be Proud

To achieve a more diverse and inclusive organization, CSIS took stock of its most significant gaps. It then created a Diversity, Equity and Inclusion (DEI) strategy and accompanying action plan to close those gaps. The DEI Strategy outlines a vision and ties collective commitments to specific actions. Overall, there are 44 commitments to pursue over the next four years. The DEI Strategy[3] is accessible to Canadians on our external website.

> **“This strategy will target behaviour and culture in addition to process and policy changes and will set bold actions in motion.”**
>
> David Vigneault
> Director of CSIS

Representative of Canadian Society

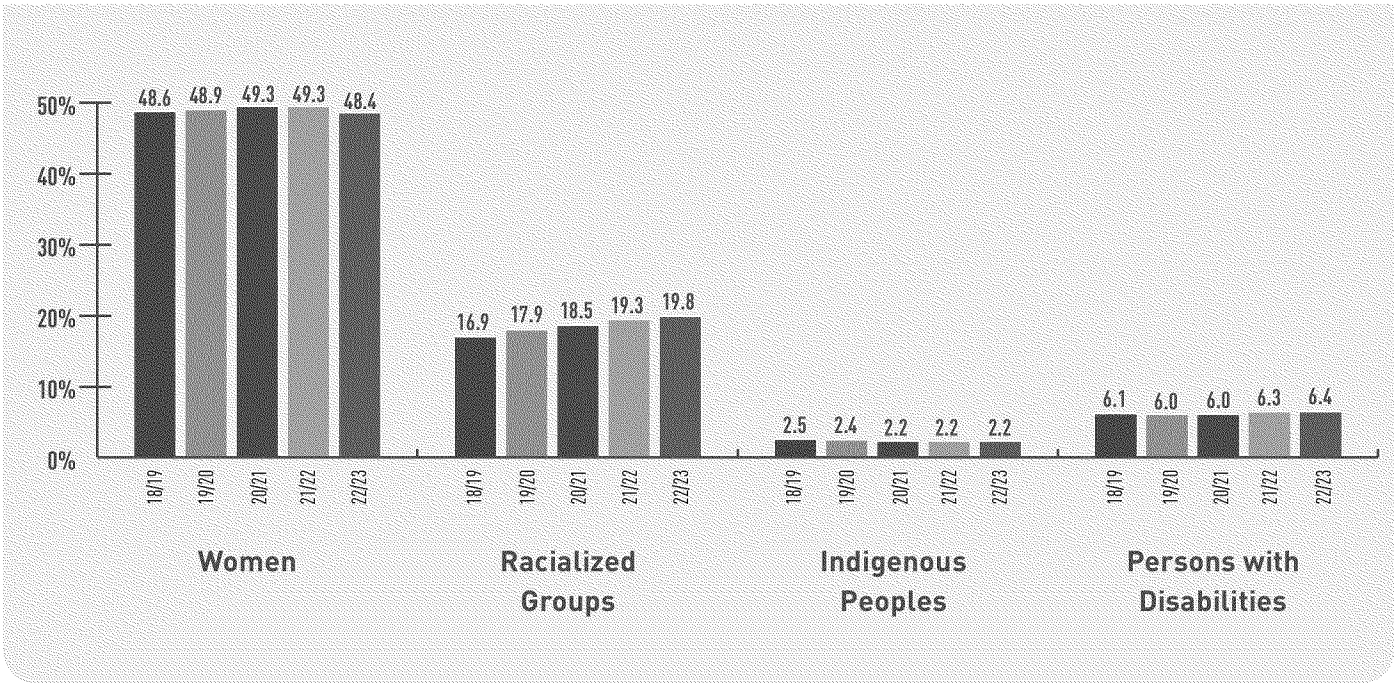
CSIS set ambitious recruitment goals meant to close representation gaps. These are aimed above work force availability (WFA) representation of racialized employees to account for ongoing growth since the last Canadian Census.

In the DEI Strategy, CSIS committed to increasing diversity in executive leadership levels. As of March 31, 2022, 21 executives self-identified as either a member of a racialized group, Indigenous Peoples and/or persons with disabilities. The rate of executives who self-identified in at least one of these three groups increased from 14% in 2021 to 21% in 2022. The most significant change occurred with persons with disabilities, where representation rose from 3% to 9%.

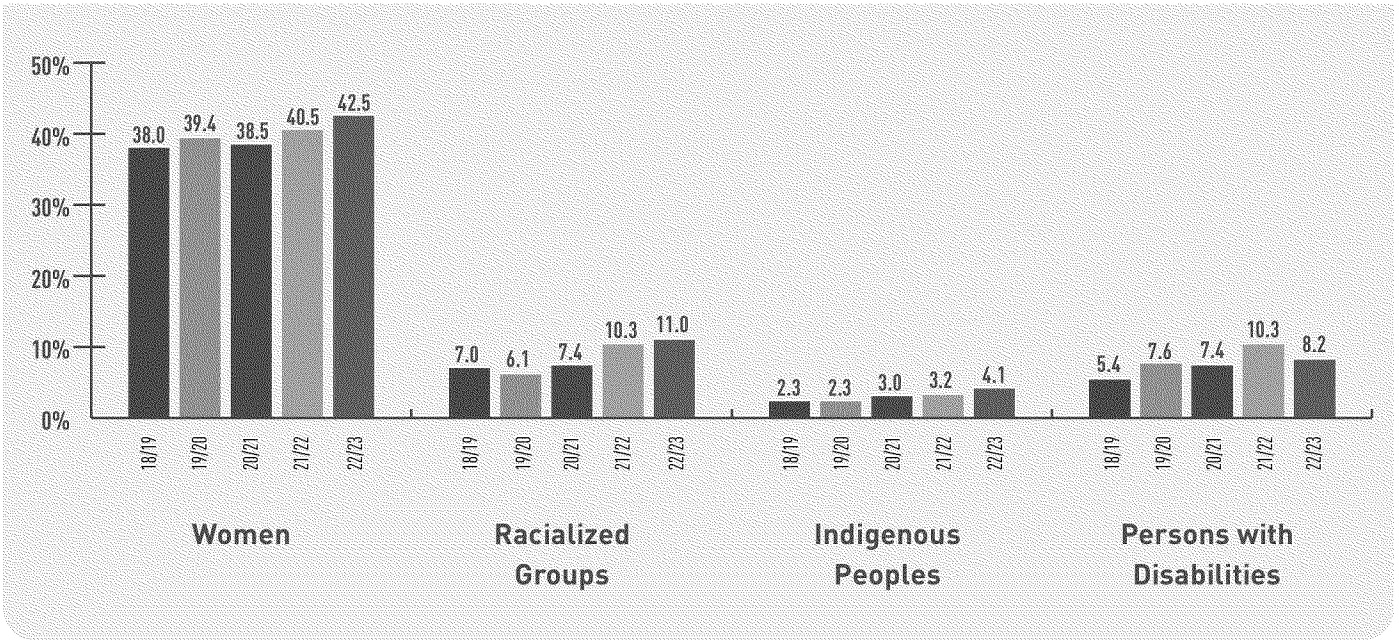
CSIS supported leadership development and career advancement for diverse employees by introducing a coaching program open to racialized and Indigenous employees, and expanding the Mentoring Program started by the CSIS Women's Network to employees with disabilities, Indigenous and racialized employees.

CSIS focused closely on recruiting to increase overall diversity in its workforce which has resulted in higher workforce participation in two underrepresented groups since 2018 – racialized employees and persons with disabilities. Indigenous participation in the CSIS workforce continues to be slightly below workforce availability, and women continue to participate on par with workforce availability, while still underrepresented in certain technical positions.

Employee Representation



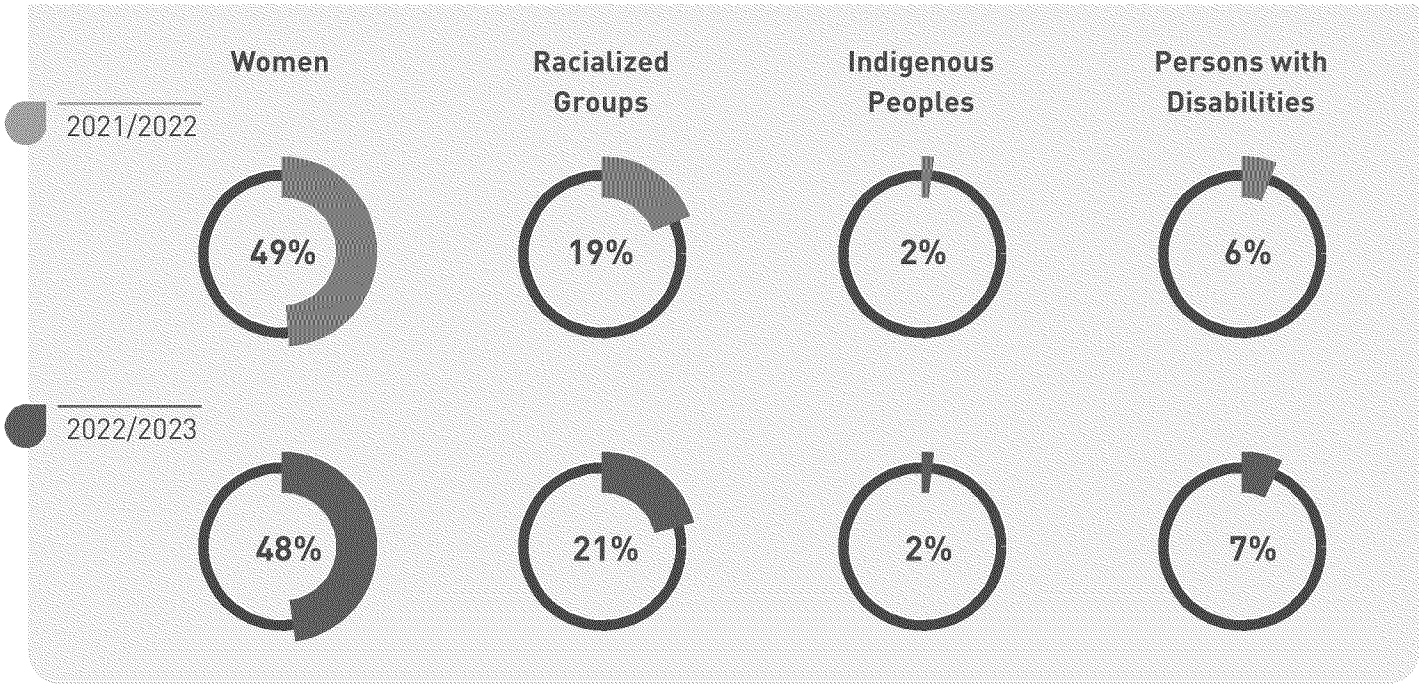
CSIS Executive Representation



Legend 2018/2019 2019/2020 2020/2021 2021/2022 2022/2023

In 2022, CSIS hired women and applicants from racialized groups at or above par with workforce availability, while continuing emphasis on attracting and hiring Indigenous applicants and persons with disabilities.

Rate of Hire



The DEI Strategy addressed barriers in HR processes. In 2022, an external review of CSIS's human resource methods was finalized. The results of the review informed recommendations in the DEI Strategy and were incorporated in a number of different tools aimed at reducing barriers and making changes to existing staffing and recruitment processes. For example, CSIS has significantly invested in Indigenous recruitment and focused recruitment efforts in highly diverse locales across Canada.

CSIS's review of its tools and methodologies brought about the implementation of strategies to:

- Eliminate barriers in communications and assessments
- Automate elements of the staffing process
- Increase transparency in the recruitment process
- Eliminate artificial barriers based on education and experience requirements for qualified candidates

Understanding Inclusion

Expanding awareness and understanding of DEI efforts, learning offerings, cultural awareness and cross-cultural sensitivity for management and employees was a prime focus this year. In 2022, CSIS's Director and senior executives concluded a year-long series of meetings with over 100 racialized and Indigenous employees, discussing matters of concern, following up to make immediate changes where feasible, and sharing the commitment of the organization to diversity, inclusion and the assurance of psychological safety. CSIS employees participated this year in over 950 DEI-related courses and seminars.

Investing in Training

A high-performing workforce is built on employee engagement, a culture of excellence, demonstrated leadership, and a healthy workplace. CSIS is constantly rethinking how we look at leadership and what learning opportunities look like for leaders at all levels.

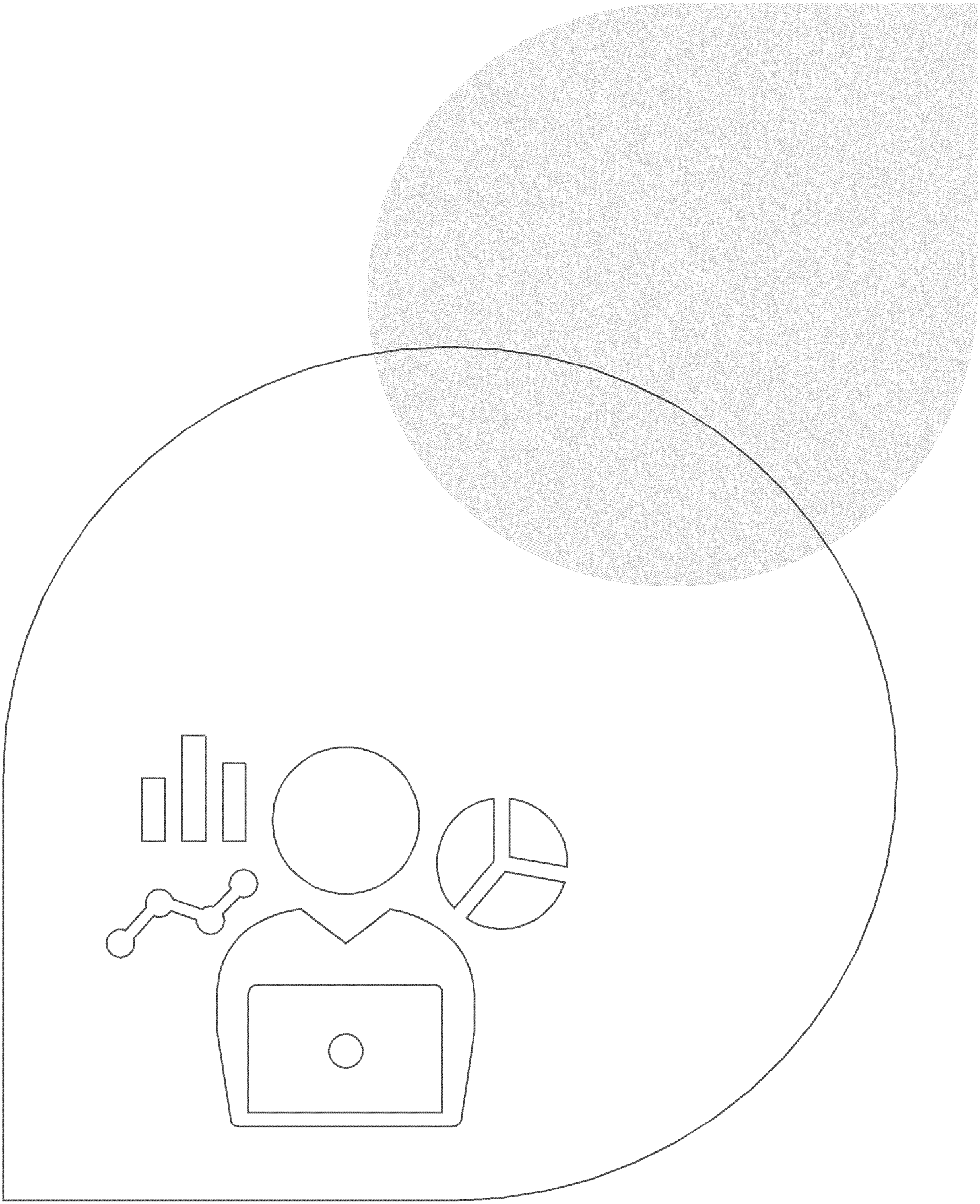
In the spring of 2022, CSIS unveiled the "Leadership Spectrum". As the name suggests, it focuses on courses and other learning opportunities related to leadership. At its core, leadership is about positively influencing those around you, which is why CSIS has created a learning framework that will provide training to leaders at all levels. The Leadership Spectrum directs employees to available learning activities to help grow their knowledge, skills and abilities in each of these areas. This program assists all employees in developing their positive influence while building a solid leadership foundation.

In the fall of 2022, CSIS unveiled the "Employee Development Journey" (EDJ). The EDJ is a virtual platform that brings together resources, tools and programs for employees to learn and develop. New resources are added continuously, including new development programs and learning paths, organized by theme and role that can be tailored to specific employees and positions.

The EDJ will:

- Promote a collaborative approach to employee development
- Develop learning paths and development programs
- Provide employees with a clear step-by-step approach to achieving their professional goals and empowering them to manage their own professional journeys
- Design tailored development programs and learning paths for CSIS's specific employment groups
- Foster a workplace culture that embraces and supports employee development and learning


EMPLOYEE
DEVELOPMENT
JOURNEY
Empowered by CSIS
Led by employees
Supported by supervisors



3

Digital and Data-Driven: **Advancing Operations for a Digital Era**

Digital and Data-Driven CSIS

Canada's adversaries exploit the current data-rich environment to target Canadian interests, intellectual property, institutions and communities. Technological developments create an increasingly complex operational landscape, in which traditional investigative techniques often have limited success. Powerful and secure communication tools are widely accessible. This evolution of the digital landscape means that most threat-related activities are now planned, discussed, orchestrated and, in some cases, realized online, in the virtual world. These threat activities spill over with real-world impacts.

As a modern, forward-leaning organization, CSIS is investing in people, training, technology, infrastructure and governance. Harnessing the power of digital platforms, data, and data-driven decision-making are all essential for future operational, corporate, and analytical success. This priority stems from internal reviews related to CSIS's data posture, grounded in the recommendations of the Report to the Clerk of the Privy Council on "A Data Strategy Roadmap for the Federal Public Service", and aligned with the themes of the Government of Canada's Digital Ambition 2022. This work also demonstrates CSIS's commitment to respond to recommendations from the Security Intelligence Review Committee made in January 2018, further to the Federal Court decision of October 2016, which call for strengthened data governance and analytical capability at CSIS.

Adopting a strategic approach to data is necessary for CSIS to fuel intelligence, to fulfill its mandate and to stay ahead of adversaries and support Canada's strategic objectives. Our approach is six-fold:

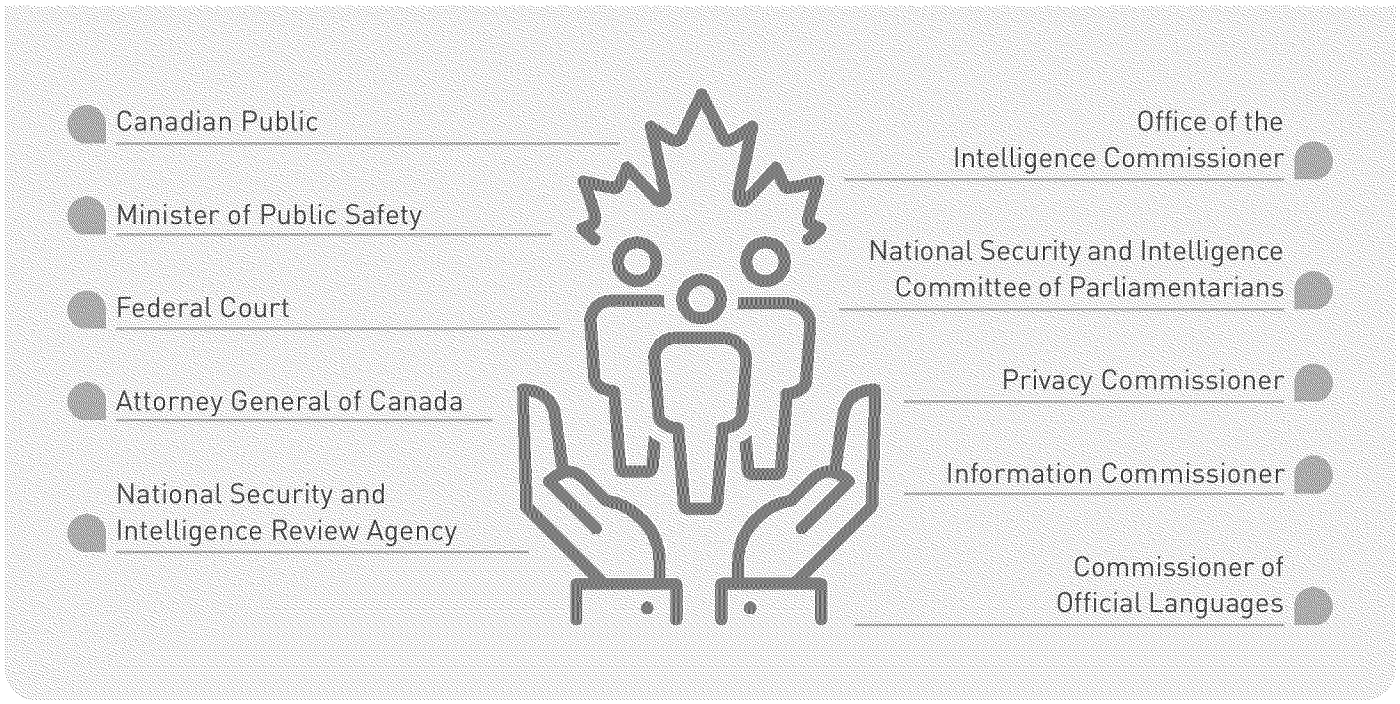
- **Data acquisition** done in a manner that is efficient and compliant with legislation.
- **Data platforms** that regroup dispersed data sources to store, organize, and manage data holdings in a modern and compliant way for further enrichment and analysis.
- **Data enrichment** enabled by leading-edge techniques, including artificial intelligence (AI) and machine learning (ML), transforming data into consumable formats.
- **Data analytics capabilities** that are automated and innovative methods that turn data into insights and intelligence while mitigating privacy risk, emphasizing ethics, and ensuring that any existing institutional biases are not replicated or reinforced.
- **Data governance** frameworks and related governing instruments that ensure rigorous compliance in the collection, use, and protection of data. This includes establishing clear data roles and responsibilities, adopting data standards, defining the proper use of technologies, incorporating diversity, equity and inclusion considerations, and fulfilling reporting and compliance requirements.

- **Data people** and mindset to build a modern and data-fueled intelligence service. An aggressive recruitment strategy of data experts is crucial in a highly competitive labour market, while an enterprise data training curriculum promotes data literacy and provides specialized training and development for data specialists.

In order to fully operate in this environment, CSIS must leverage technology to counter the systemic hostile activities by foreign state actors, emerging threats and unanticipated crises. Federal Court decisions interpreting CSIS's foreign intelligence assistance mandate have highlighted a technological gap. Practical experience interpreting new dataset authorities reveals significant limitations in CSIS's ability to operate in a data-rich landscape. CSIS requires modern and nimble authorities to perform its duties and functions in a way that accommodates technological evolution and the speed with which threats develop, while also maintaining *Charter*-protected rights in accordance with the rule of law.

Accountable to Canadians

Accountability



Making DEI Part of our Business

The DEI Strategy commits to the integration of DEI principles into CSIS's business. The organization integrated DEI considerations and commitments into standardized training and information sessions for new Intelligence Officers and Executives; piloted and implemented customized Gender Based Analysis (GBA) PLUS interactive training; and incorporated GBA PLUS considerations in its formal evaluation processes. CSIS initiated a GBA PLUS review of certain security screening assessments. Resources were provided to employees on how to apply the GBA PLUS lens in their work and CSIS strongly encourages application of GBA PLUS lens to all activities. Various business strategies, policies, decisions and business approaches were examined with diverse employee networks before being finalized, and their input integrated into final plans.

Transparency

CSIS remains steadfast in its efforts to increase public awareness, engagement, and access to national security information. CSIS shares information about its priorities and activities with Parliament, stakeholders, partners, media, and the general public on a daily basis.

CSIS has committed to diligently and respectfully forging ahead towards building trust with communities across the country. Through a better understanding of our respective needs, we will meet our common goal of protecting our country and all its people.

Responding to the National Security Transparency Advisory Group (NS-TAG) Report

In May 2022, the National Security Transparency Advisory Group (NS-TAG) published a report on "How National Security and Intelligence Institutions Engage with Racialized Communities." In CSIS's response to the report, it committed to providing additional information on the activities and outcomes of the stakeholder engagement program.

Created in 2019, CSIS's national stakeholder engagement strategy was to engage directly with those whose interests we serve and do it with senior-level representation. In order to build and foster strong relationships with stakeholders, the program openly interacts with Canadians in key sectors of Canada's civil society and economy. Learning from each other's experiences helps foster a collective understanding of Canada's broad national security interests and priorities.

The objectives of engaging with non-government stakeholders—including those in Canada's diverse, marginalized and racialized communities—include:

- Enhancing trust by speaking as candidly as possible about CSIS's mandate and activities
- Sharing how CSIS understands and analyses the threat landscape
- Supporting accountability
- Supporting transparency
- Attracting and retaining a diverse and inclusive workforce
- Effectively fulfilling CSIS's mandate to ensure that all Canadians recognize CSIS as being responsive to their interests as they relate to national security
- Learning how we can engage and support them

Approach

The stakeholder engagement team's approach is to reach out directly to stakeholders and partners with a clear and transparent offer to initiate a dialogue. The ethos of the program is one of listening, offering support to increase collective resilience against national security threats, and finding common interests and foundations for partnership and collaboration.

Raise Awareness

Sharing as much information as widely as possible builds understanding across Canada of the threat environment and supports informed dialogue on national security issues. This objective is achieved in part by offering information on CSIS's public website[4] and social media accounts; delivering public remarks; appearing before Parliamentary committees; media interviews; disseminating a bi-weekly newsletter which highlights publications; events; and other open-source items related to Canada's broad national security interests.

Build Resilience

When a stakeholder identifies concerns relating to possible threat-related activity, the stakeholder engagement team can connect them, upon request, with operational colleagues for further investigation. As appropriate, CSIS connects government partners with stakeholders and partners to ensure that their perspectives and priorities are considered in policymaking, service delivery, and funding decisions. CSIS's advice to the Government of Canada on security issues is also informed, in part, by its stakeholder engagement activities.

CSIS routinely engages with a variety of stakeholders, including elected and public officials at all orders of government, to discuss the threats to the security and interests of Canada posed by foreign interference within the current limitations of the *CSIS Act*. As part of this engagement, CSIS provides defensive briefings regarding specific threats.

Inform Operations

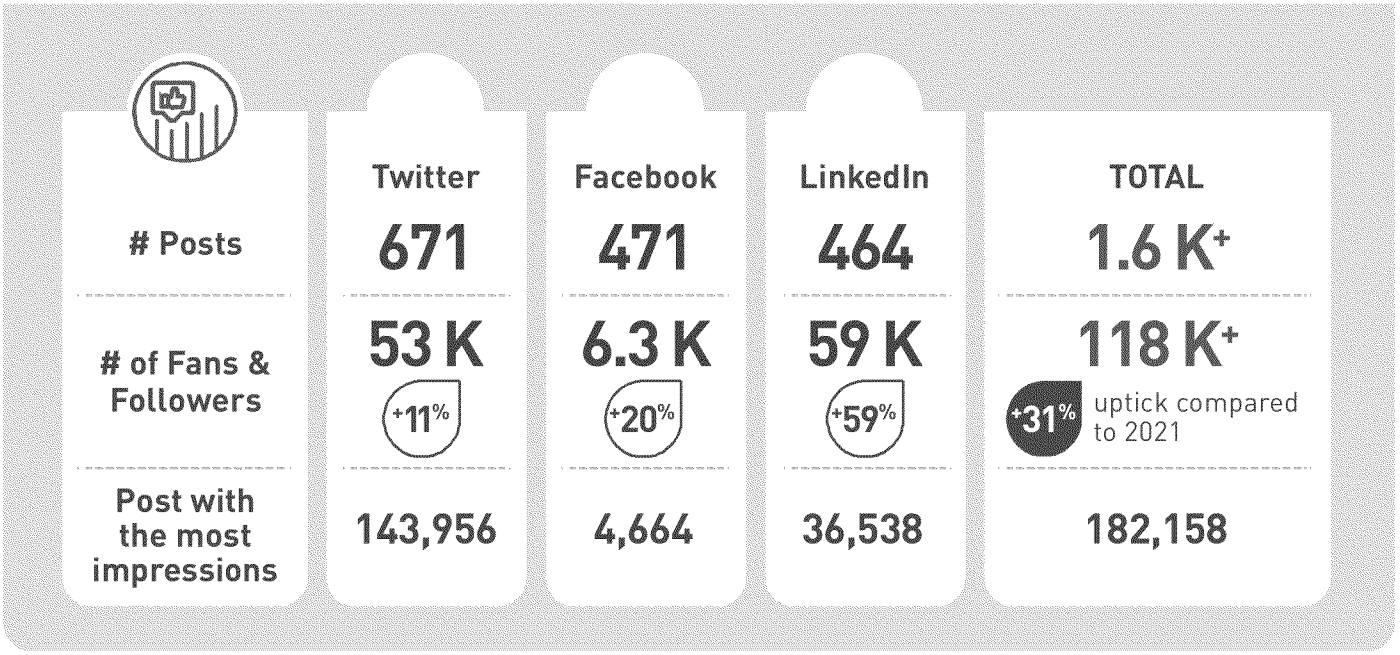
Stakeholders provide CSIS with an important understanding of their priorities, perspectives, and concerns. This information is used to help inform operational activities and CSIS's own internal policies and practices, including those related to diversity, equity, and inclusion. This can be particularly important for the organization's interactions with racialized and equity-deserving communities. Engagement outcomes and lessons learned are shared with colleagues at CSIS headquarters and in Regional Offices across Canada. The stakeholder engagement team maintains strong connections with Regional Liaison teams across Canada to ensure that there is a cohesive approach to all of CSIS's public-facing activities.

Guide Policy-Makers

When stakeholders identify concerns or offer recommendations or considerations, these help CSIS to better understand the impacts of our national security investigations and activities, including perceived gaps. This input informs CSIS as it adapts its policies, programs and operations, and is critical as it examines the need for *CSIS Act* modernization. CSIS's advice to Government is also informed by stakeholder inputs, which demonstrate the real-world impacts of national security threats. CSIS's information and advice can therefore assist the Minister and the government in making decisions that are responsive to the perspectives and priorities of stakeholders.

CSIS on Social Media

Through social media platforms, CSIS endeavours to communicate transparently about our decision-making processes and national security activities. In 2022, CSIS published 1,600 posts across all social media platforms. CSIS's posts were seen over 180,000 times in total. With over 118,000 followers overall, CSIS has its largest social media presence ever on Twitter. The audience following CSIS on social media has steadily grown, achieving a 31% uptick compared to 2021.



Access to Information

CSIS's Access to Information and Privacy (ATIP) activities contributes to CSIS's transparency efforts by balancing the public's right of access to information with the legitimate need to protect sensitive national security information and maintain the effective functioning of government. The *Access to Information Act* (ATIA) and *Privacy Act* provide Canadians, as well as individuals and corporations present in Canada, the right to access federal government records. CSIS prides itself on providing excellent service and proactively promoting transparency.

For the 2022 calendar year, the **on-time compliance rates** stood at **95%** for the Privacy Act requests and **92%** for the ATIA requests.

1,246 ***Privacy Act*** **requests** received in 2022 (8% increase over 2021)

1,218 ***Access to Information Act*** **(ATIA) requests** received in 2022 (53% increase over 2021)

1,274 Informal requests received in 2022 (49% increase over 2021)

Parliamentary Review

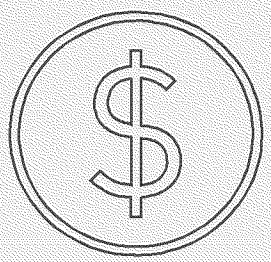
Canadians rightfully expect Canada's national security and intelligence agencies to operate in an ethical and transparent manner while keeping our country safe. In 2022, CSIS appeared a record 14 times in front of Parliamentary committees. This provided CSIS Executives with an opportunity to testify, in an open setting, on a number of different topics including foreign interference, IMVE, Islamophobia, the *Investment Canada Act* and critical minerals, to name a few. CSIS also testified before the Public Order Emergency Commission to provide information on the role CSIS played in the broader Government of Canada response to the Freedom Convoy protests in 2022.

CSIS has often voiced the need for a robust and informed national security dialogue, and public appearances—such as those in front of Parliamentary committees—provide a forum to share important information about these threats to all Canadians.

At its core, national security is about protecting people, and to be effective, CSIS needs the trust and help of the Canadian public. CSIS recognizes that in order to better understand and combat today's complex and evolving security threats we must engage directly with those whose interests it serves, including those from Canada's racialized communities, religious minority communities, and Indigenous Peoples. Upcoming opportunities to hear from Canadians, such as the statutory review of *Bill C-59, the National Security Act, 2017*, are ways for Canadians to help shape the future of national security legislation in Canada. With a renewed dialogue on national security in Canada, CSIS looks forward to hear from Canadians on potential avenues for modernizing its authorities.

Expenditures 2022

	2019/2020	2020/2021	2021/2022
Salaries*	$372,348,794	$417,615,370	$404,107,049
Operating	$238,736,299	$259,284,331	$238,065,778
TOTAL	**$611,085,093**	**$676,899,701**	**$642,172,827**



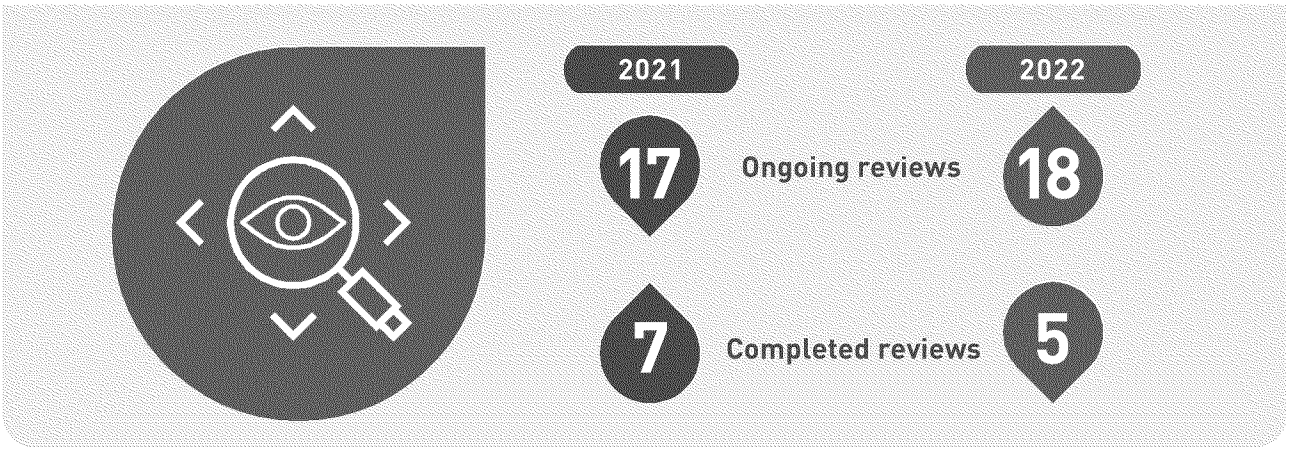
* Salary costs include Employee Benefits Payments

Review and Compliance

CSIS has been subject to external review since its inception in 1984. The creation of the National Security and Intelligence Committee of Parliamentarians (NSICOP) in 2017 provided, for the first time, a forum for parliamentarians to discuss and review classified material. The creation of the National Security and Intelligence Review Agency (NSIRA) in 2019 enabled an independent body to review the national security and intelligence activities of multiple federal departments and organizations, in addition to CSIS. In parallel, CSIS has developed an internal operational compliance program to promote compliance with legislation, ministerial direction and operational policies.

External review and operational compliance are core features of CSIS's transparency and accountability framework. They are essential to maintaining the trust and confidence—of the Federal Court, review and oversight bodies, parliamentarians and, ultimately, Canadians—that CSIS is effectively exercising its authorities in compliance with the law. Review and compliance reports and recommendations help ensure CSIS remains a learning organization that strives for continuous improvement. This results in positive changes to the processes and culture of our organization. Review bodies' public reports also help inform discussions with Canadians about national security issues and the role of national security agencies, in an ever-evolving threat environment.

Number of reviews by NSIRA and NSICOP



In 2022, CSIS continued to implement a new *Operational Compliance Framework* and to develop and update policies and procedures so that employees have clear guidance on how to exercise CSIS's authorities in a compliant manner. CSIS has also created an *Operational Technology Review Committee* to identify and assess compliance risks with the use of innovative techniques and emerging technologies in support of operational activities.

CSIS reviewed 65 reports of potential non-compliance in 2022, compared to 98 instances in 2021. These numbers reflect the inherent challenges of maintaining operational compliance within an evolving technical and legal landscape. However, they also reflect efforts to foster a culture of compliance across the organization. CSIS employees are increasingly familiar with the compliance program, as they proactively report instances of potential non-compliance and proactively seek advice related to issues of potential concern.

As part of CSIS's commitment to the duty of candour to the Federal Court, in 2022 CSIS continued to disclose any instances of warrant-related non-compliance to the Federal Court. CSIS also proactively advised the Federal Court, the Minister of Public Safety and NSIRA on issues of non-compliance pertaining to Canadian law, Ministerial Direction and potentially unlawful activity. In 2022, as part of NSIRA's annual review, CSIS began providing quarterly updates to NSIRA on compliance issues.

In 2022, CSIS continued to engage with external review bodies on a broad range of reviews. Some related specifically to CSIS, including an annual review of the use of TRMs, and horizontal reviews implicating CSIS and multiple departments, such as the annual reviews on the implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act (ACMFEA)* and the *Security of Canada Information Disclosure Act* (SCIDA).

Perhaps the most notable NSIRA review published in 2022 was the review arising from Federal Court Judgment 2020 FC 616, also known as the *en banc* matter, which yielded 20 recommendations. CSIS responded publicly to these recommendations, and has undertaken extensive work to address many of the issues examined through recommendations of a former Deputy Attorney General. To reflect the seriousness in which CSIS takes this review, CSIS has created a dedicated project team to coordinate implementation of the recommendations.

CSIS strives to maintain a strong and constructive working relationship with review bodies and is committed to meeting its obligations related to access, engagement and the provision of information. Review and compliance are fundamental and complementary parts of the learning culture at CSIS. The results of external and compliance reviews often point to areas in which ambiguity in the *CSIS Act* creates legal and compliance risk.

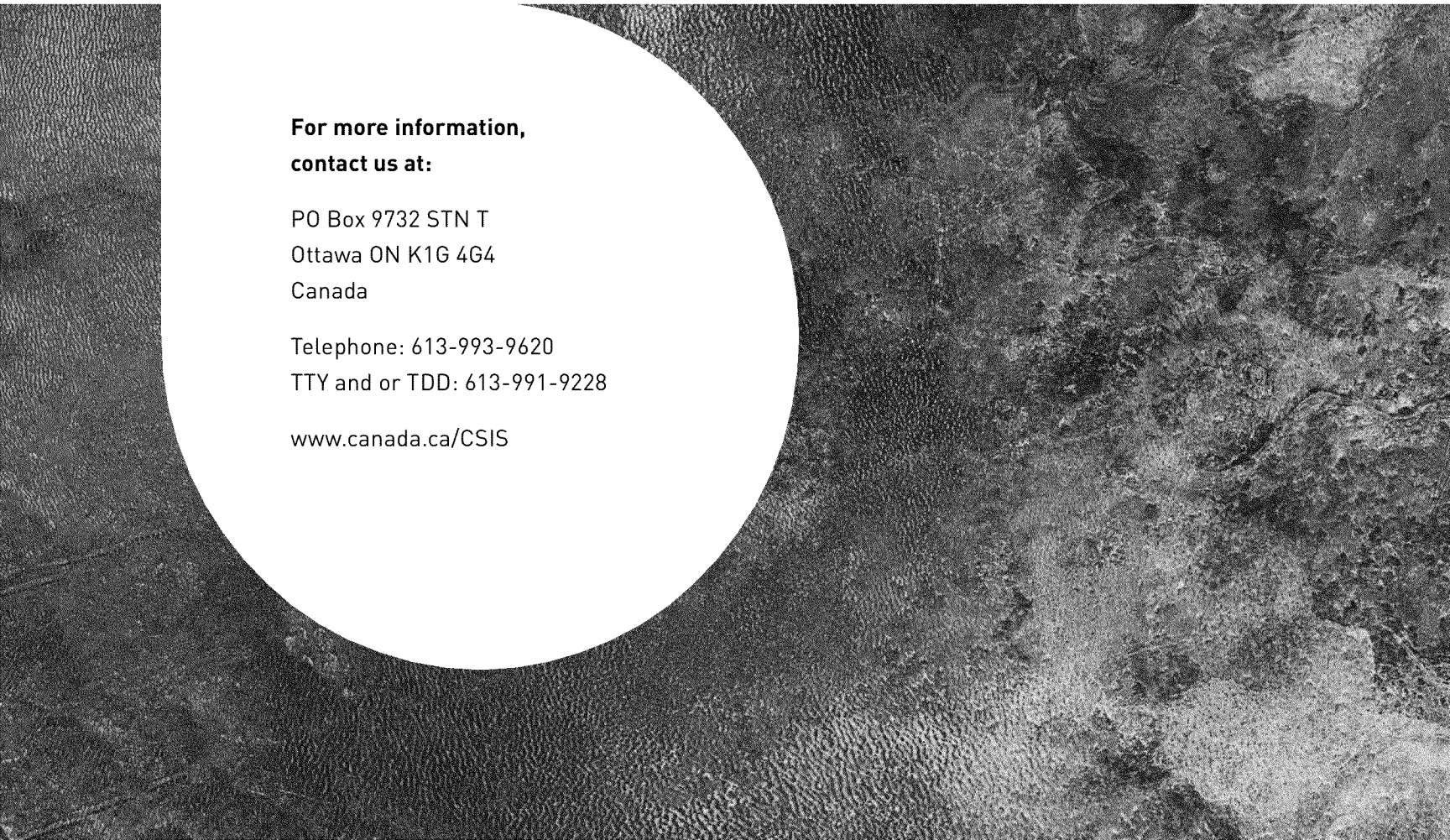
CSIS employees are dedicated to the mission and are proud to be transparent and accountable for their work in keeping Canada and Canadians safe, while safeguarding the sources and methods that make it possible. CSIS is not a secret organization but must work in secret.

Conclusion

The people of CSIS are focused on the mission to protect Canada's prosperity, national interests and the safety of Canadians. CSIS will continue to build a work culture and a workplace grounded in trust and mutual respect that attracts and retains Canada's best and brightest employees. Building on the best of our existing tradecraft and skills, CSIS will equip itself with the capabilities, competencies and agility needed to fulfill its shared mission as a global, modern, forward-leaning intelligence organization. CSIS will invest widely in people, training, technology, infrastructure and governance to harness the power of digital platforms, data, and data-driven decision-making, all of which are essential for future operational, corporate, and analytical success.

Web Links

1. https://www.canada.ca/en/security-intelligence-service/corporate/publications/pnspac-en.html
2. https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-and-you/foreign-interference-and-you-list.html
3. https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-diversity-equity-and-inclusion-strategy-2022.html
4. https://www.canada.ca/CSIS



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

www.canada.ca/CSIS