



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

© His Majesty the King in Right of Canada, as represented by the Minister of Public Safety, 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	7
Message from the Director of CSIS	11
Mission Focused: Addressing the Threat Environment	17
Duties and Functions	18
CSIS Responds	19
Foreign Interference	20
Espionage	21
Economic and Research Security	22
Cyber Threats	23
Violent Extremism	24
Counter-Proliferation	25
Security Screening	26
Threat Challenges Ahead	28
Increasingly Polarized World and Ideologically Motivated Violent Extremism	28
Misinformation / Disinformation	29
The Indo-Pacific	30
Ukraine – Protracted Conflict	30
Arctic and Northern Canada	30
Afghanistan	31
Russian Private Military Contractor – Wagner	31
Security Implications of Returning Canadian Extremist Travellers (CETs)	31

Engaging with Canadians	32
Outreach in 2022	32
CSIS across Canada	34
Advancing Truth and Reconciliation	35
Integrated Terrorism Assessment Centre (ITAC) Profile	36
People First: Investing in our Workforce to Deliver our Mandate	39
Diversity, Equity and Inclusion	40
A Diversity, Equity and Inclusion (DEI) Strategy of which to be Proud	40
Representative of Canadian Society	41
Understanding Inclusion	43
Investing in Training	44
Digital and Data-Driven: Advancing Operations for a Digital Era	47
Digital and Data-Driven CSIS	48
Accountable to Canadians	51
Making DEI Part of our Business	52
Transparency	53
Responding to the National Security Transparency Advisory Group (NS-TAG) Report	53
CSIS on Social Media	55
Access to Information	55
Parliamentary Review	56
Review and Compliance	57
Conclusion	59



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**

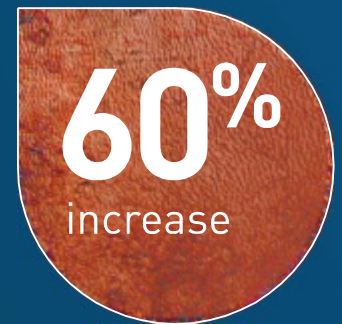
Provincial **26**

Municipal **17**



PEOPLE FIRST

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



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.



ACCOUNTABLE TO CANADIANS



Access to Information and Privacy (ATIP)

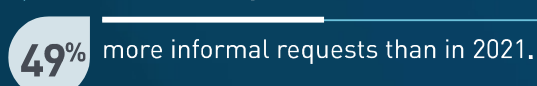
1,246 *Privacy Act* requests received in 2022



1,218 *Access to Information Act (ATIA)* requests received in 2022



1,274 *Informal requests* received in 2022



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



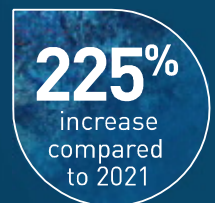
Number of reviews by National Security and Intelligence Review Agency (NSIRA) and National Security and Intelligence Committee of Parliamentarians (NSICOP)



Social Media Analytics



Record Number of Parliamentary Appearances







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.

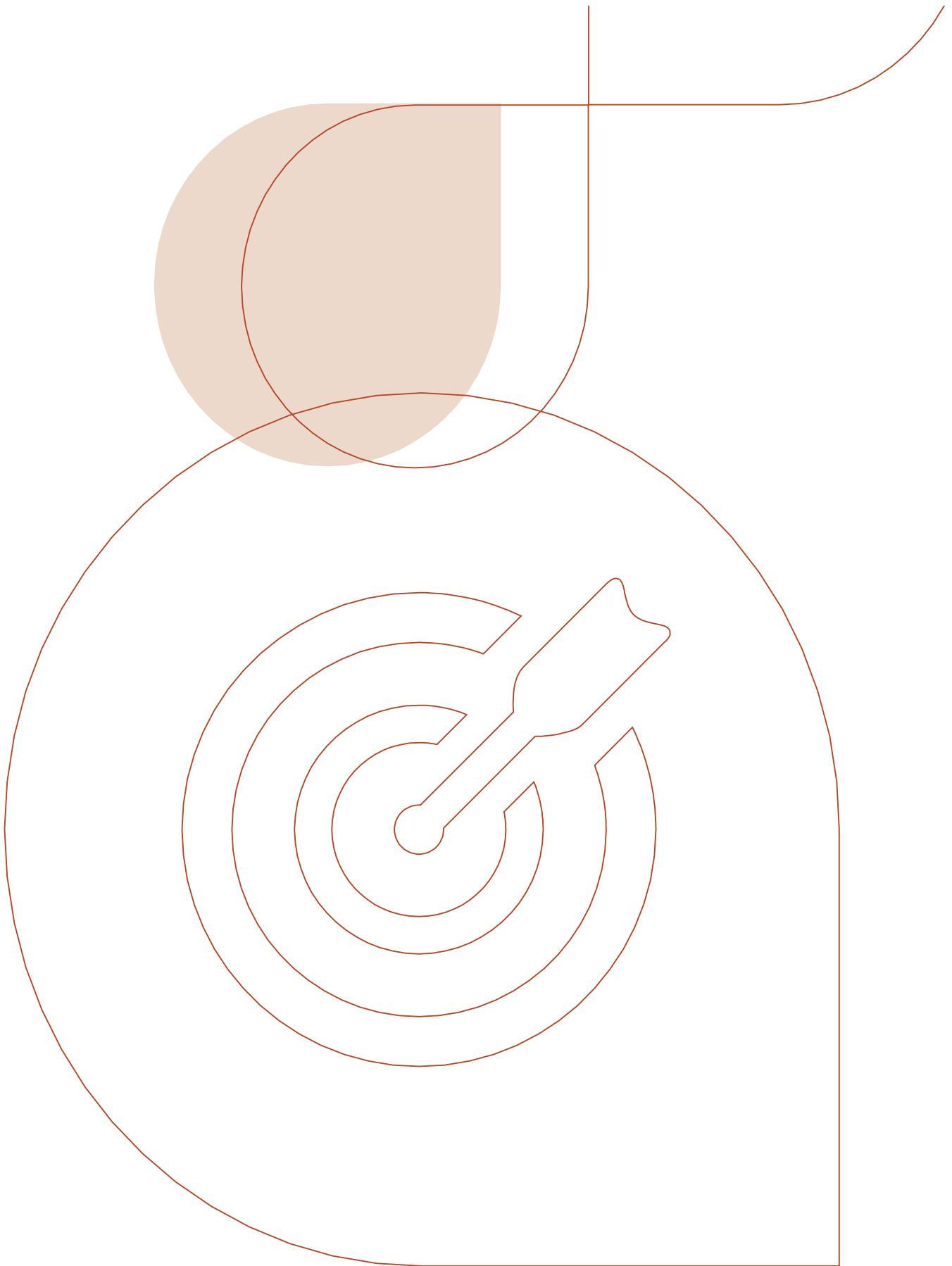
The threats to our country continue to accelerate. I am confident that the people of CSIS will work with our partners to tackle them head-on to keep Canadians safe, secure and prosperous, into 2023 and beyond.

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. ”



The background is a complex, textured pattern of red, orange, and blue. A large white circle is cut out from the center, containing the title text. The text is arranged in three lines: "Mission Focused:" in a smaller font, "Addressing the Threat" in a larger, bold font, and "Environment" in a larger, bold font. The text is in a dark red or brown color.

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.

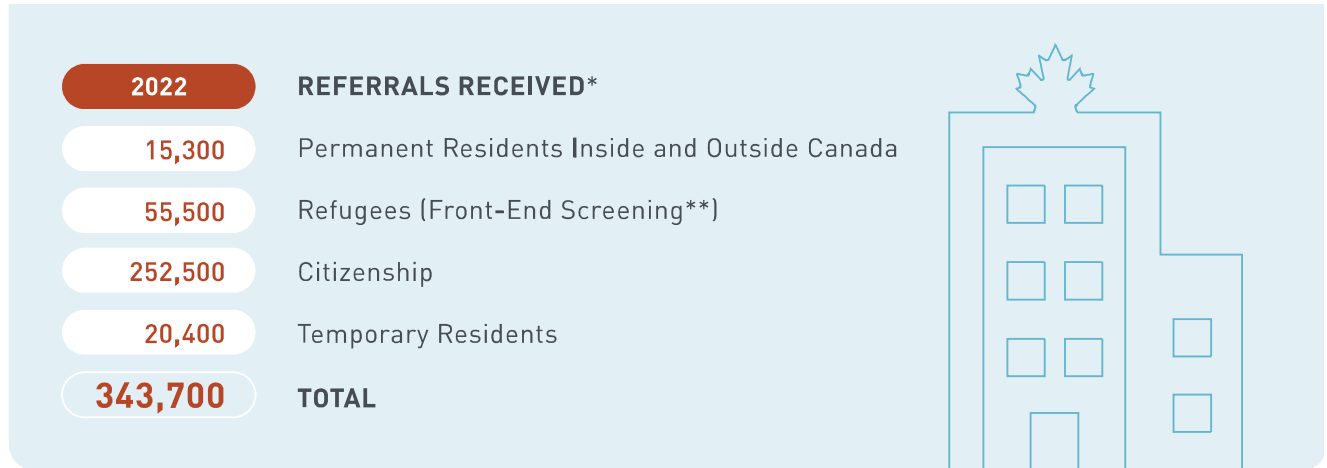
GSS also conducts screening to protect sensitive sites—including airports, marine, and nuclear facilities—from national security threats. Furthermore, it assists the RCMP in vetting Canadians and foreign nationals who seek to participate in major events in Canada. Finally, GSS provides security assessments 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.

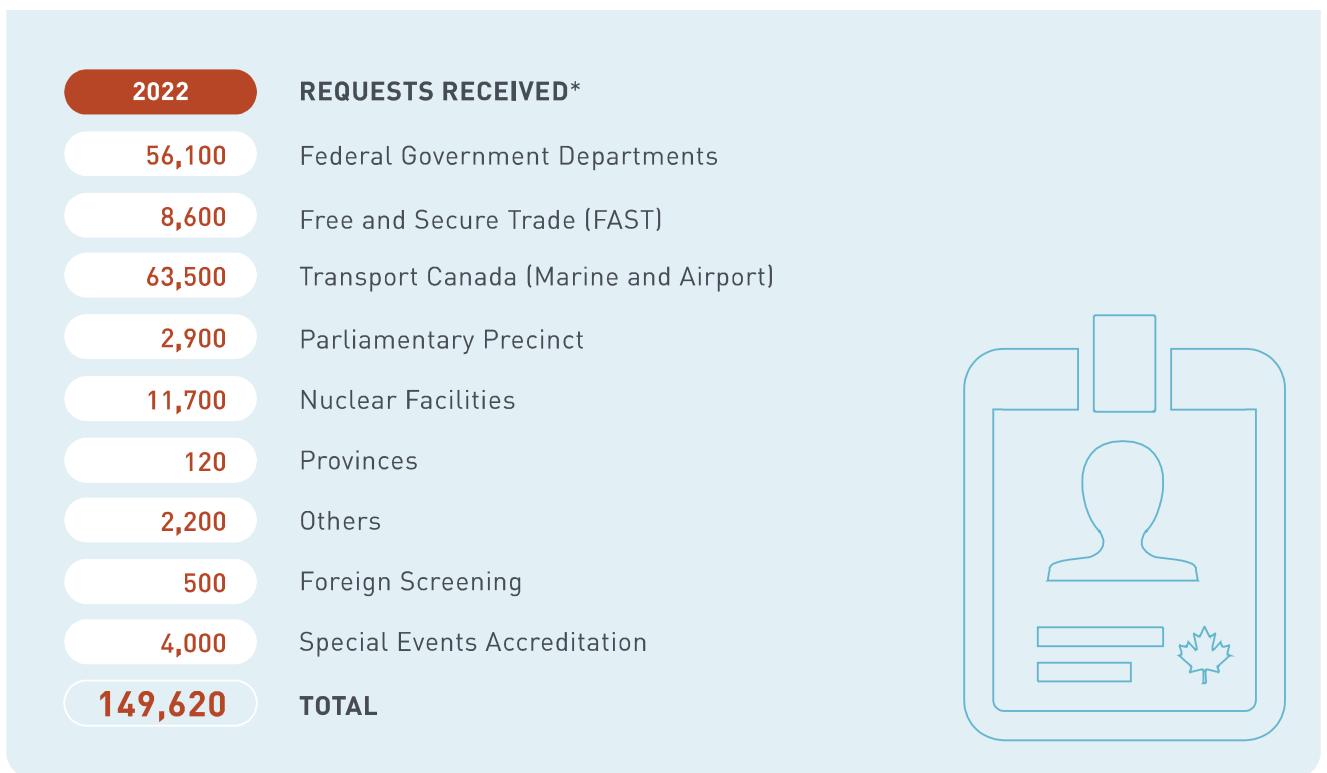
As part of this, CSIS continues to screen applicants from Afghanistan, referred by IRCC, as part of the Government of Canada's commitment to resettle at least 40,000 Afghan refugees by the end of 2023. The completion of inadmissibility screening is a regular part of the review process for resettlement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



Government Screening Programs



*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.

MISINFORMATION

is false or inaccurate information that is spread regardless of intent to mislead.



DISINFORMATION is false or inaccurate information created deliberately with a malicious intent to manipulate a narrative. Misinformation becomes disinformation when hostile actors weaponize it for political influence and interference.

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 Faso has increased, and Wagner continues to expand Russian influence and undermine Western interests.

Wagner is likely applying known strategies such as 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

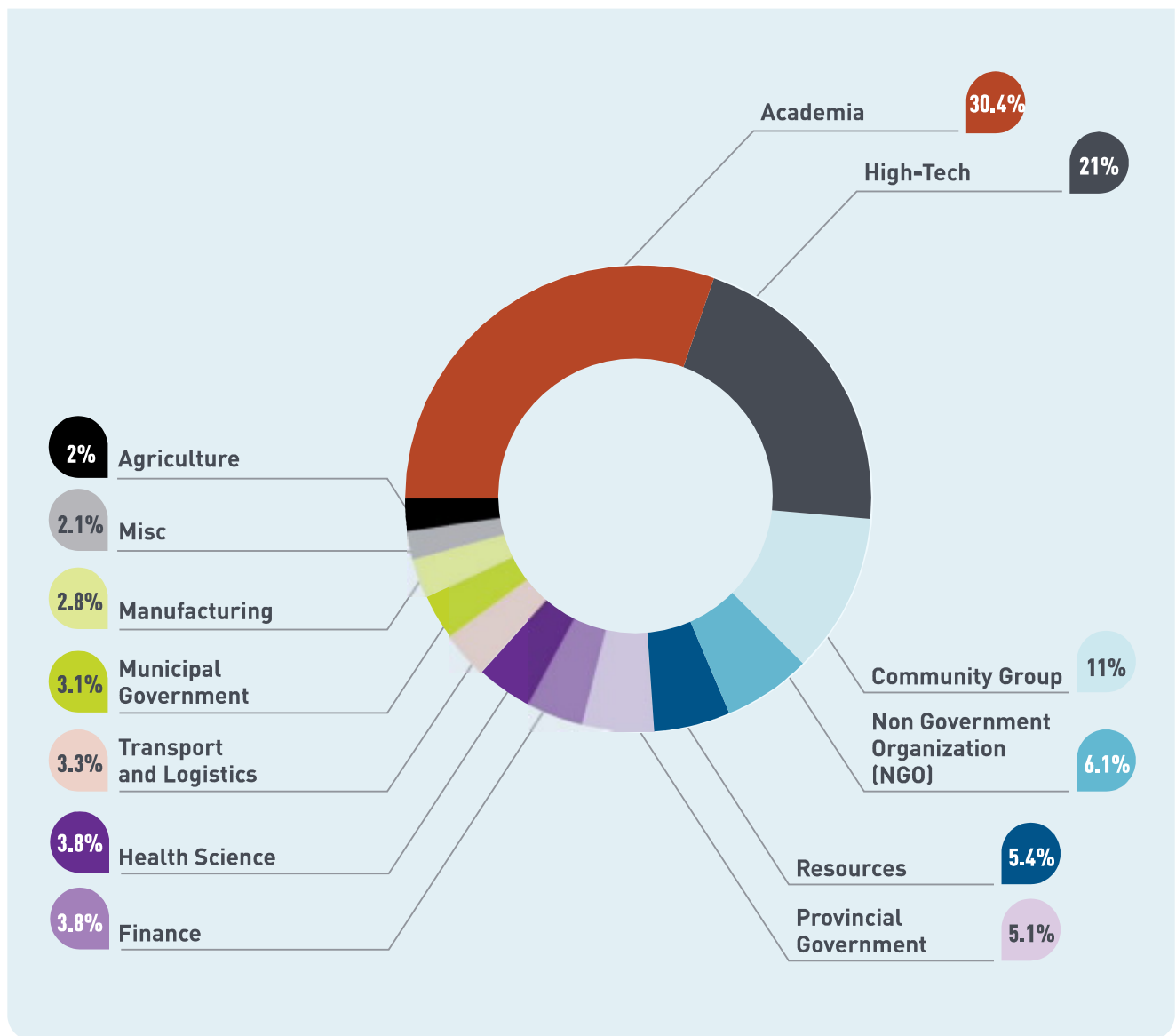
Outreach in 2022

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

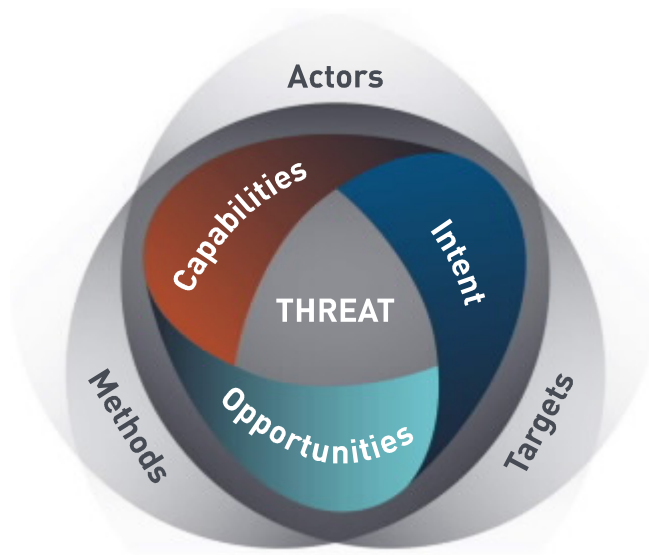
The Integrated Terrorism Assessment Centre (ITAC), created in 2004, was established to independently produce comprehensive threat assessments using a wide range of classified and unclassified sources. ITAC serves as a “community resource” to support government decision-making and provide timely analyses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

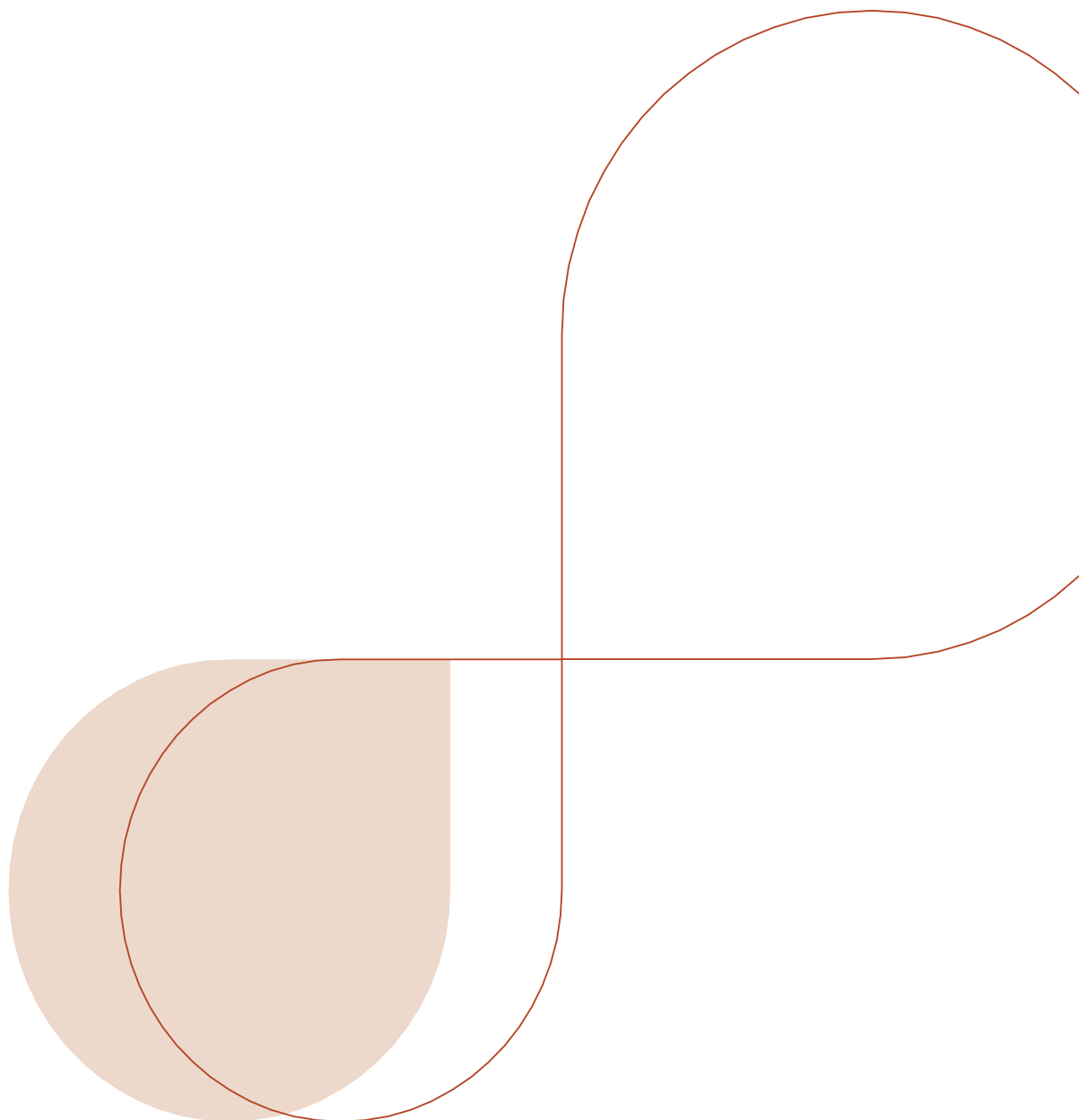
ITAC’s threat assessments are based on a rigorous methodology that analyzes quantitative and qualitative indicators pertaining to the intent, capability and opportunity of potential threat actors to conduct an act of terrorism. These assessments serve several functions, including raising awareness of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

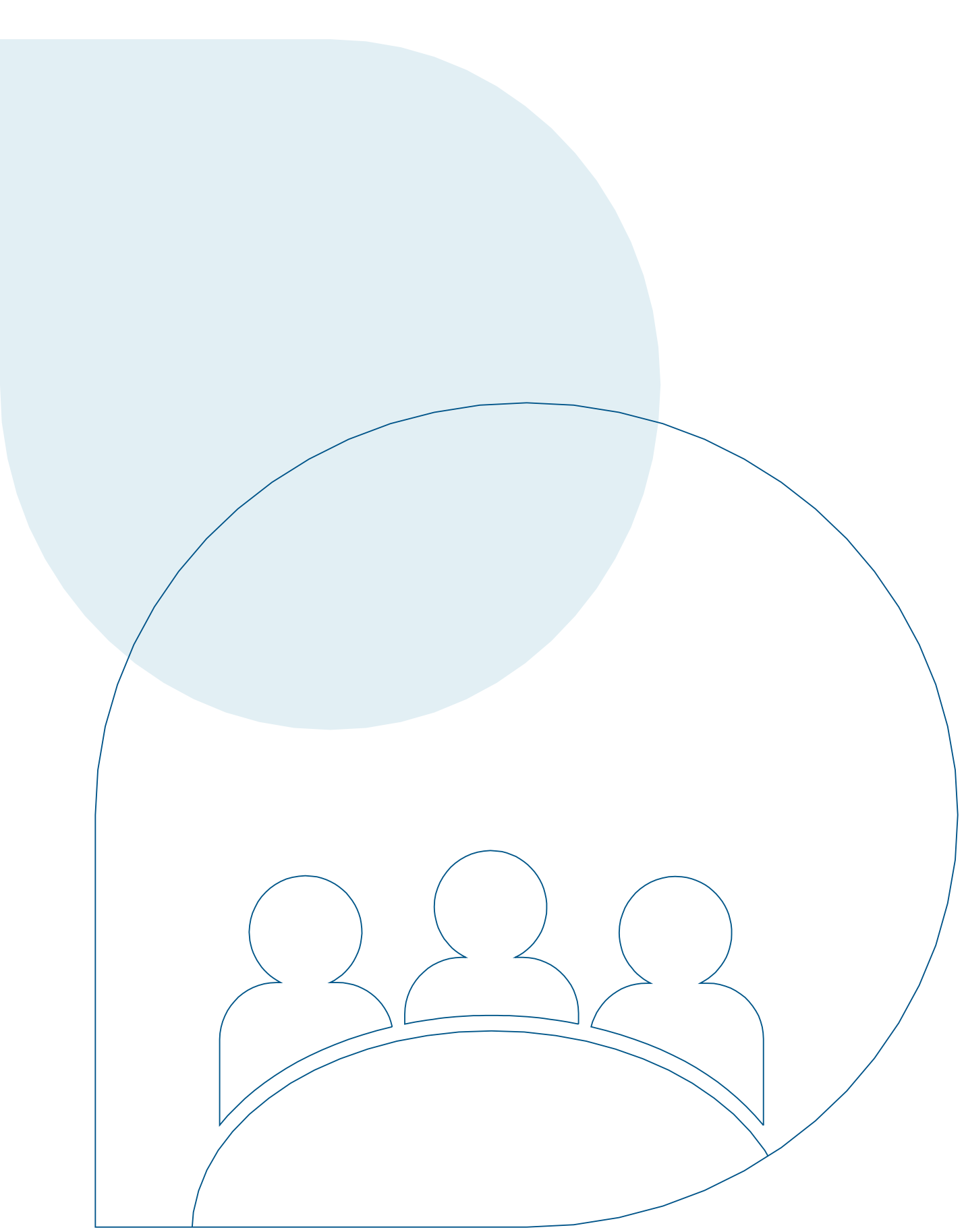


ITAC has a very broad dissemination mandate. Beyond senior government officials and federal security partners, it disseminates reports to provincial, territorial and municipal law enforcement agencies, as well as to critical infrastructure stakeholders.

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.







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

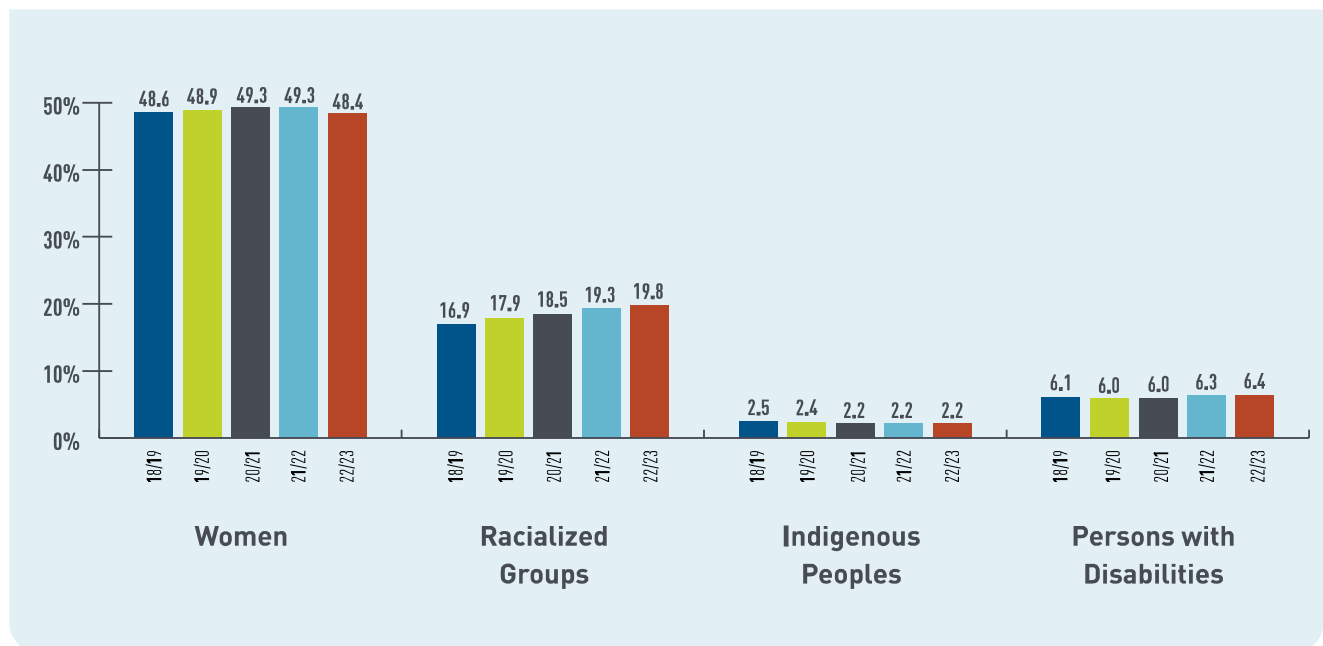
CSIS set ambitious recruitment goals meant to close representation gaps. These are aimed above work force availability (WFA) representation of racialized employees to account for ongoing growth since the last Canadian Census.

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.

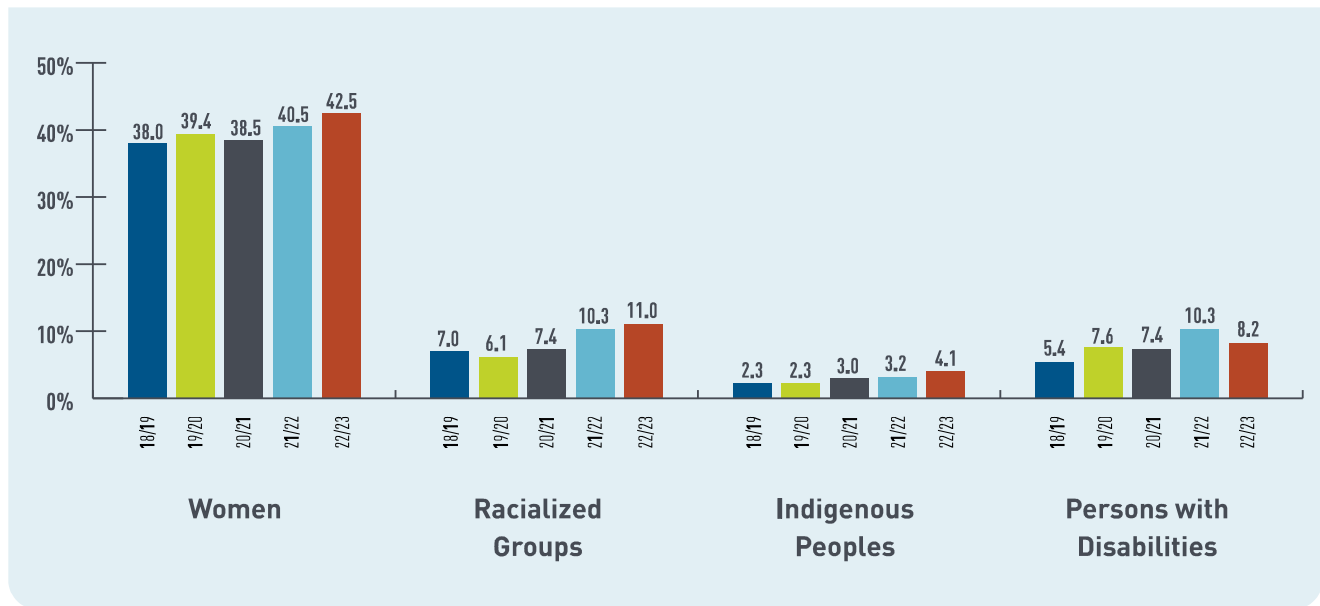
Employee Representation



Legend

- 2018/2019
- 2019/2020
- 2020/2021
- 2021/2022
- 2022/2023

CSIS Executive Representation

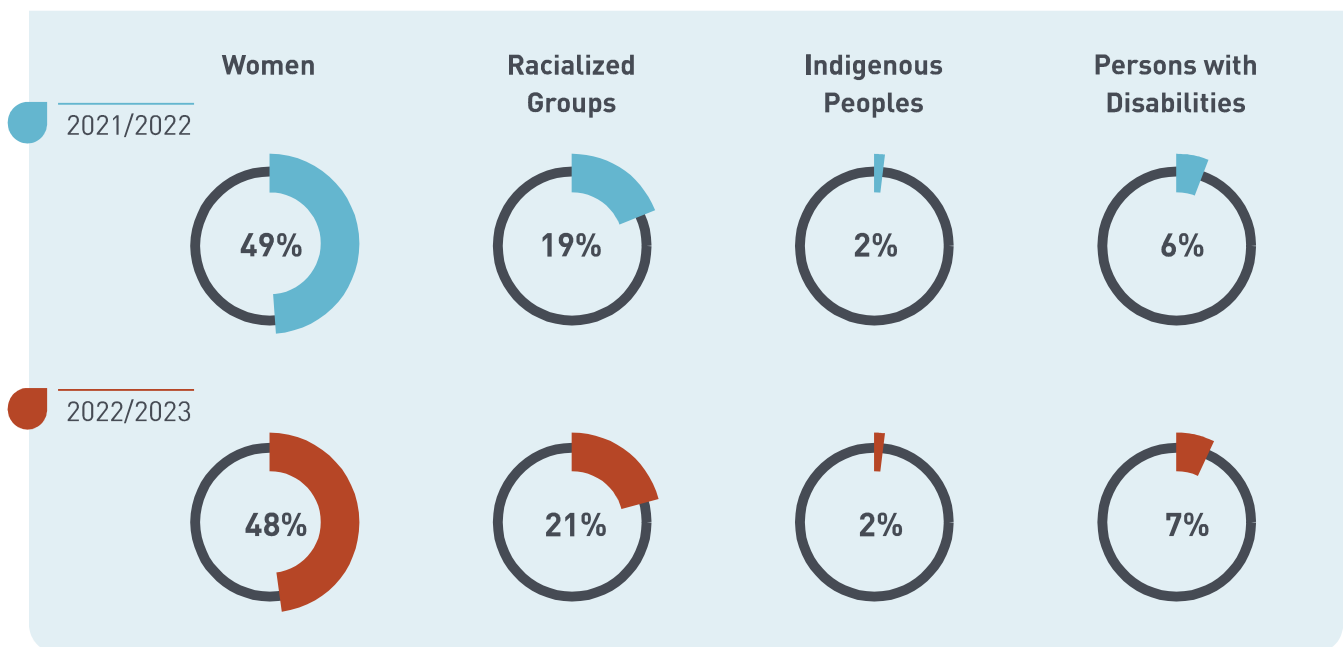


Legend



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

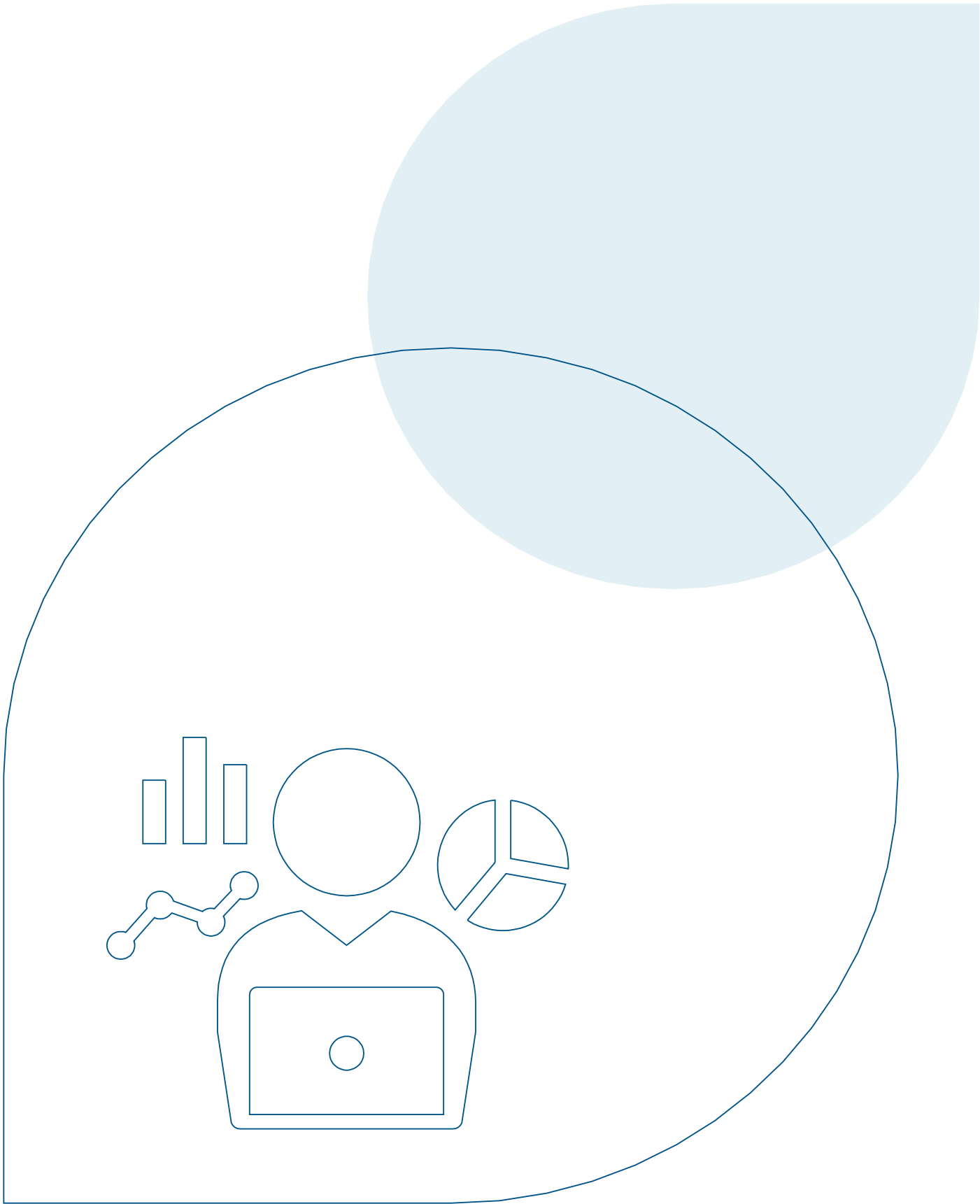
EMPLOYEE DEVELOPMENT JOURNEY

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.

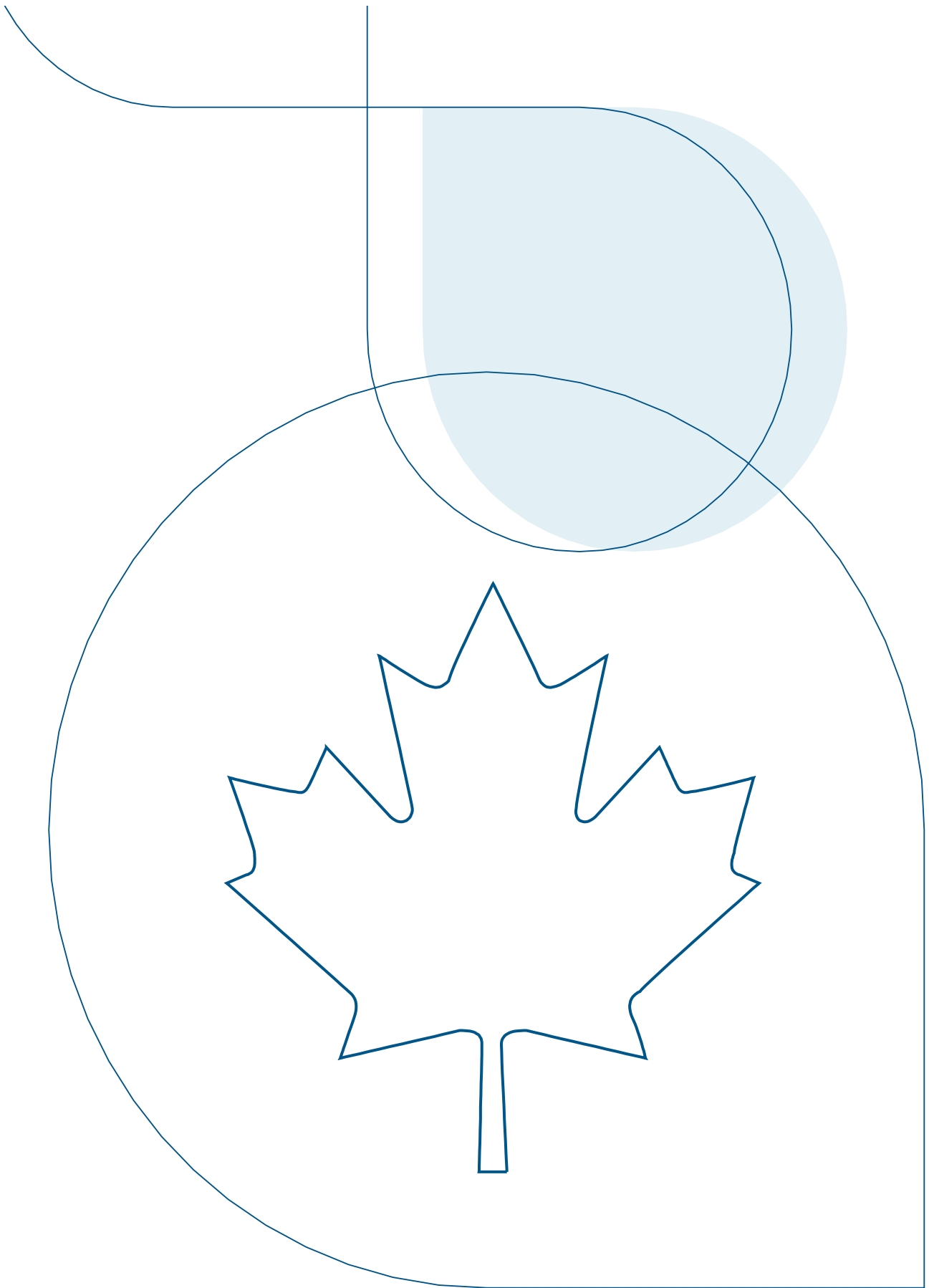
As a modern, forward-leaning organization, CSIS is investing in people, training, technology, infrastructure and governance. Harnessing the power of digital platforms, data, and data-driven decision-making are all essential for future operational, corporate, and analytical success. This priority stems 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.



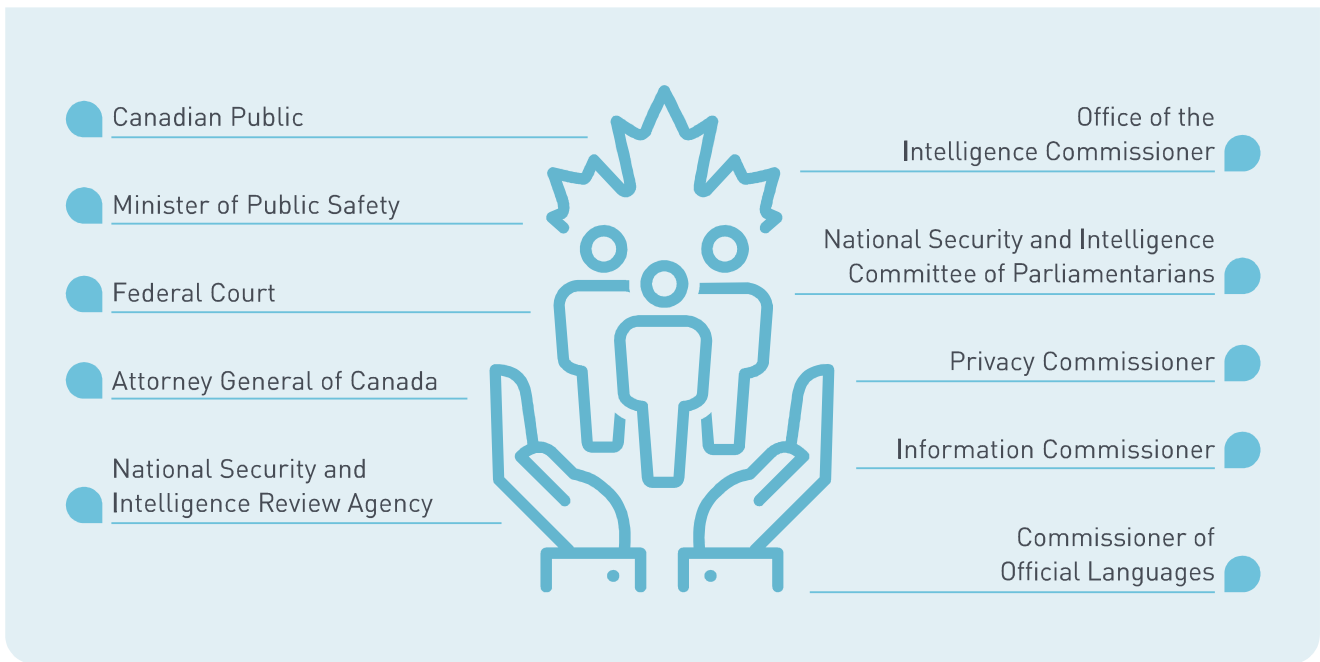


4

**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

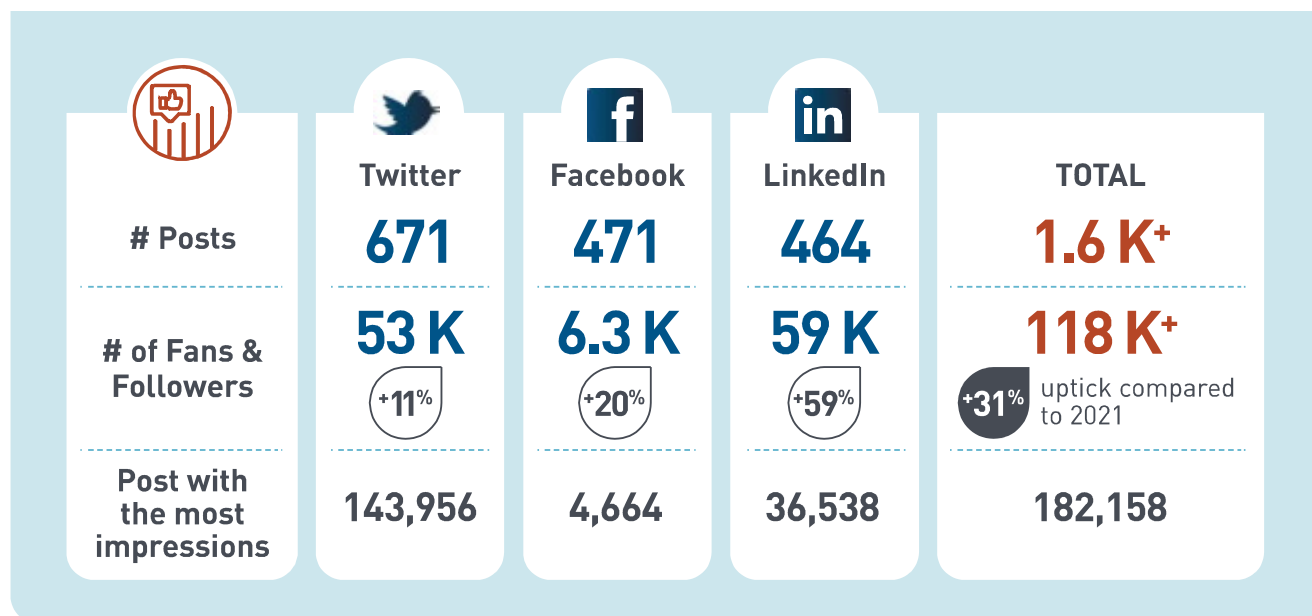
Stakeholders provide CSIS with an important understanding of their priorities, perspectives, and concerns. This information is used to help inform operational activities and CSIS's own internal policies and practices, including those related to diversity, equity, and inclusion. This can be particularly 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

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)

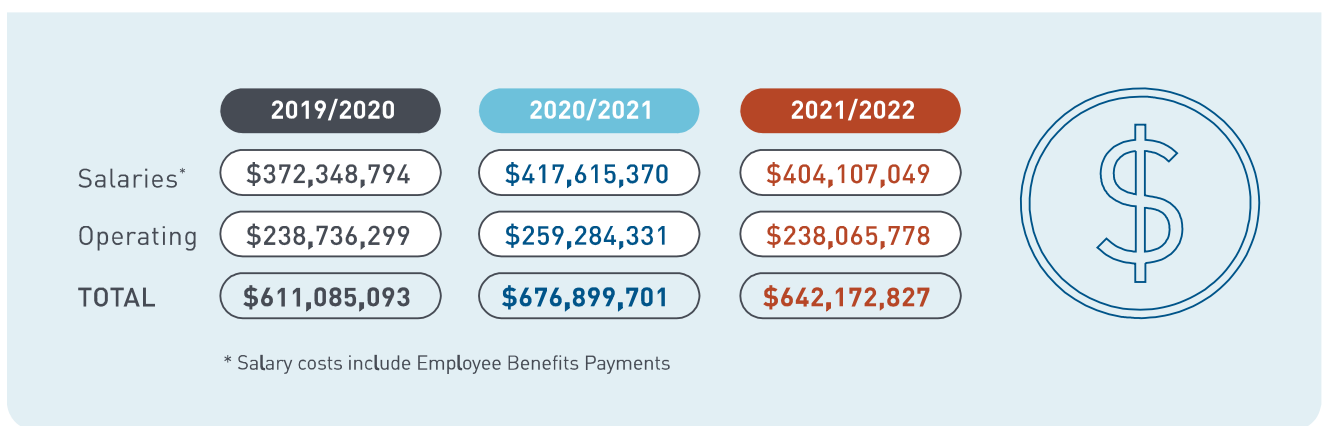
Parliamentary Review

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

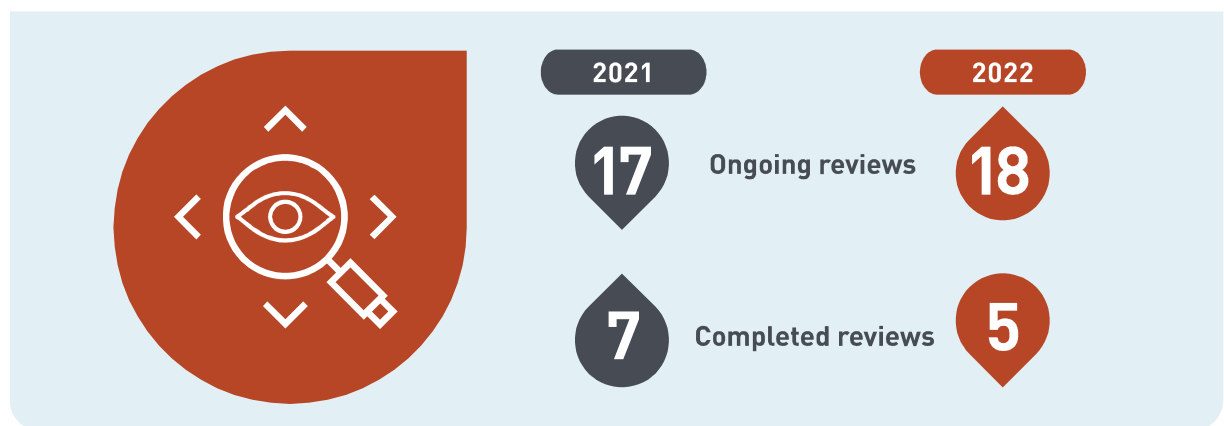


Review and Compliance

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



Canadian Security
Intelligence Service

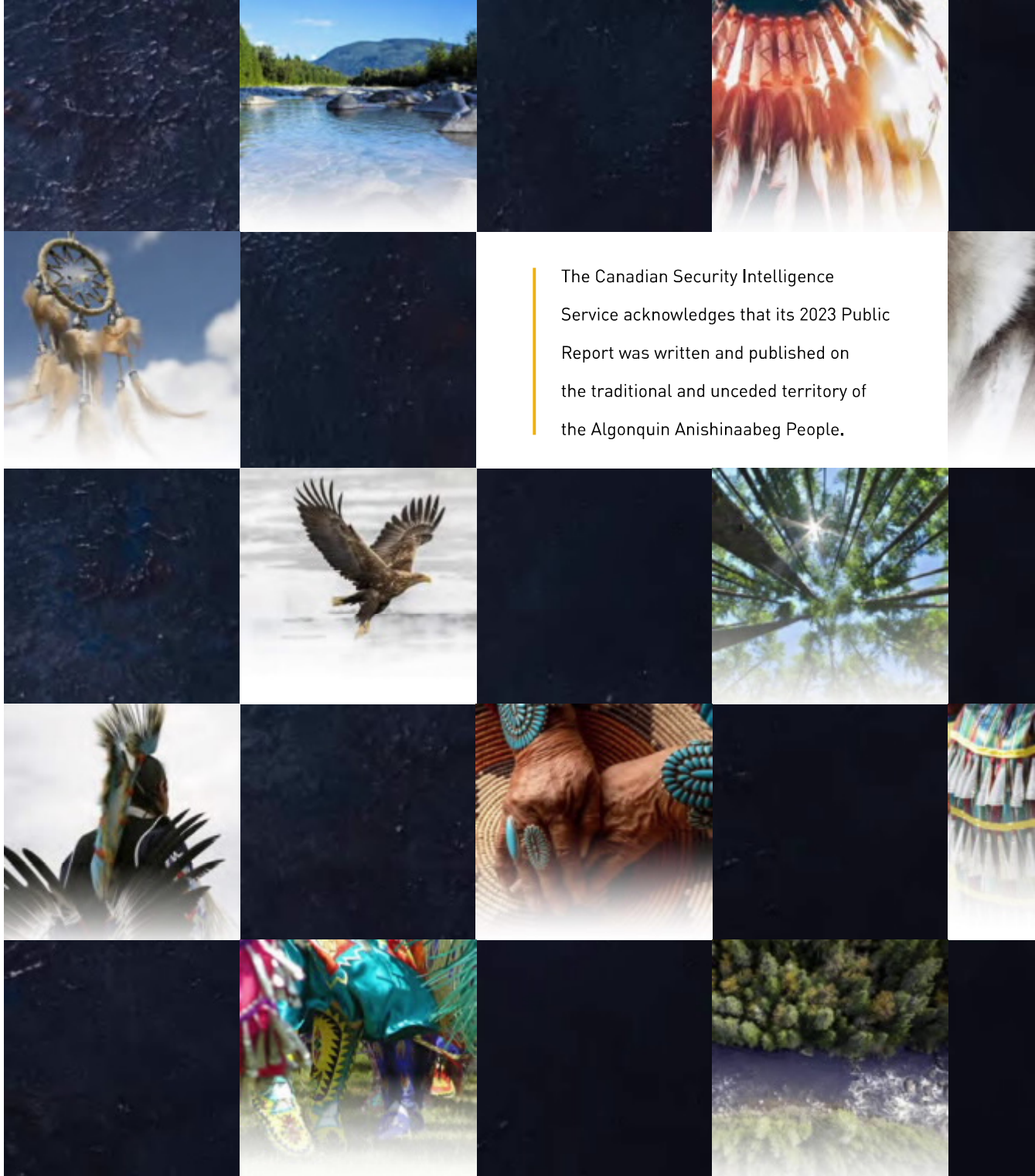
Service canadien du
renseignement de sécurité



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



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.

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

© His Majesty the King in Right of Canada, as Represented by the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs, 2024.

Table of Contents

Message from the Director of the Canadian Security Intelligence Service	6	Key Ideologically Motivated Violent Extremist Events in 2023	45
Year in Review: A Significant Period for National and International Security	8	Politically Motivated Violent Extremism	47
National Security in 2023	12	Religiously Motivated Violent Extremism	47
Highlights	16	Working in Partnership to Reduce the Violent Extremism Threat	48
Mission Focused: Confronting the Threat Environment	22	Security Screening	50
Duties and Functions	24	Integrated Terrorism Assessment Centre	52
Threat Reduction Measures in 2023	25	2023 Trends and Looking Ahead	52
CSIS' Role in National Security Investigations	25	Partner Focused: Engaging with Canadians and Partners	54
Operating in an Increasingly Complex Threat Environment	26	Shining the Light: Building a Strategic, Transparent, and Accountable CSIS	56
Foreign Interference and Espionage	28	Building Partnerships through Engagement	60
The People's Republic of China	29	Academic Outreach	60
The Russian Federation	30	Partner Engagement	61
The Islamic Republic of Iran	31	Policy and Accountability	64
India	31	The Arctic and Northern Framework	64
Using Social Media to Warn Canadians	32	The Indo-Pacific Strategy	65
CSIS Responds	32	Consulting Canadians: <i>CSIS Act</i> Consultations	65
Economic and Research Security	34	External Review and Oversight	66
Prioritizing Research Security in the Five Eyes	35	Justification Framework	66
Counter Proliferation	36	People First: A Workplace for All	68
Cyber Threats	38	People First: In Pursuit of a Better CSIS	70
CSIS' Role in Cybersecurity	38	Workplace Initiatives	74
Cybersecurity and Geopolitics	39	Diversity, Equity, and Inclusion Strategy	74
Information Warfare	39	CSIS 2023–2025 Accessibility Plan	74
Ransomware	39	Increasing Diverse Representation	75
State-based Cyber Threats	40	Employee Engagement through Networks and Committees	75
Focus on Cyber: Navigating AI Technologies	42	CSIS Cares – Government of Canada Workplace Charitable Campaign 2023	76
Violent Extremism	44	Addressing the Unauthorized Disclosure of Intelligence	78
Ideologically Motivated Violent Extremism	44	Conclusion	80

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



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.

”



David Vigneault
Director of the Canadian Security Intelligence Service

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.

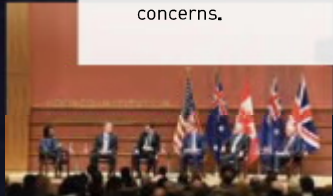
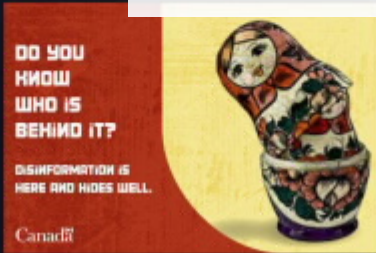
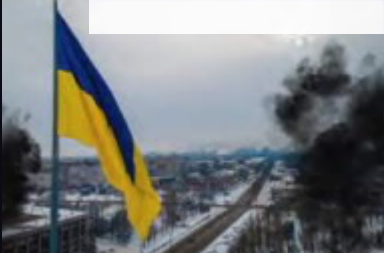
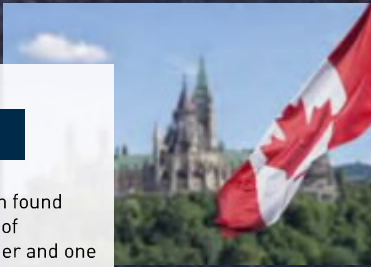
The year 2023 presented significant challenges, and CSIS employees stepped up during this extraordinary year to meet them while truly representing the best of Canada. I am tremendously grateful for their tireless efforts and dedication to the protection of Canada’s national security, prosperity, interests,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

One Mission. One CSIS. One Canada. ■

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:

149,620



Investment Canada Act (ICA)

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

1,010



CSIS Partnerships

Domestic Arrangements

79 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
- Research and innovation institutes
- Academia
- Community organizations
- Provincial, territorial, and municipal governments
- Civil society and advocacy associations



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.**

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

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



ACCOUNTABLE TO CANADIANS



CSIS on Social Media

X f in @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)

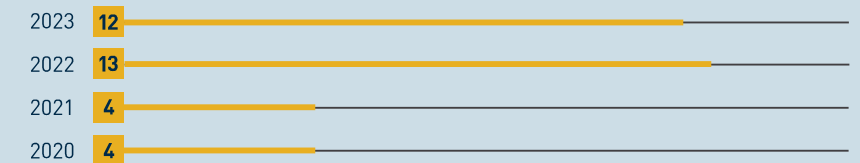


Ongoing reviews **17** Completed reviews **2**

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



Parliamentary Appearances



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



“

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.

who challenge their narrative. They have more options and opportunities to conceal their threat activities, including by using criminal organizations as proxies.

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.

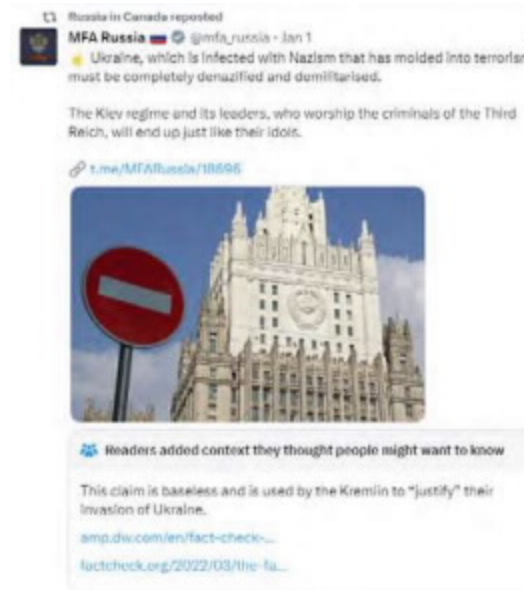
CSIS assesses that the PRC and CCP organizations will remain an enduring threat to Canadian information, technology, democratic institutions, and diaspora communities. The PRC will use a variety of methods, including public engagement, media outreach, and promotional campaigns, as well as deceptive and 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. ■

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.

Saskatchewan River Delta, Manitoba.

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 unremediated 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.

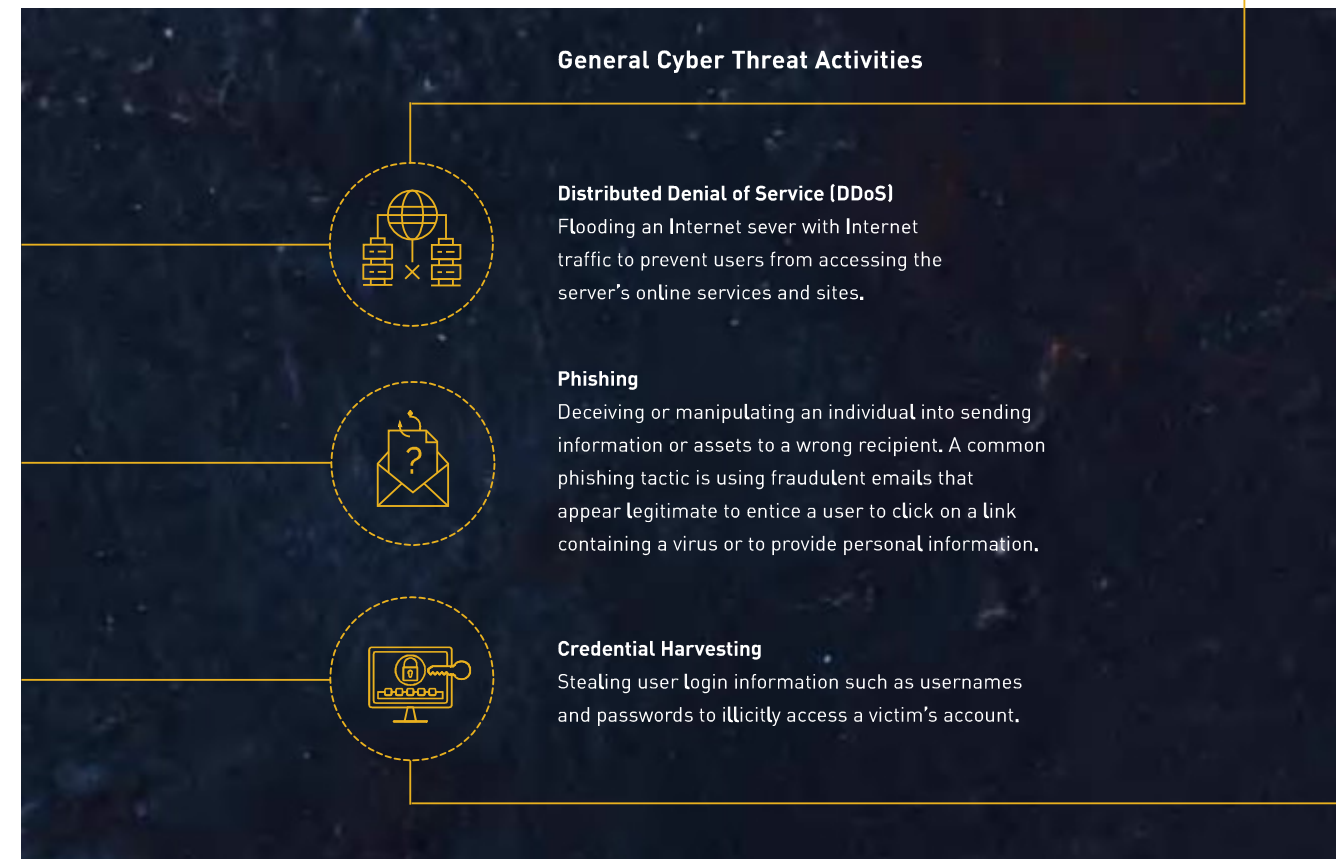
Iran

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. ■



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.

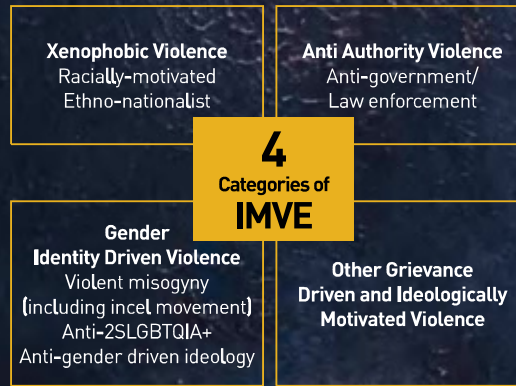
The attack appears targeted and while Villalba-Aleman held various ideological grievances, his primary motivation was likely his anti-gender views. The alleged perpetrator's actions appear driven by a desire to express his grievances and send a message to his perceived enemies. CSIS assesses that the

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



2022
6 RMVE Arrests



2023
16 RMVE Arrests

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 7, 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 8, 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.

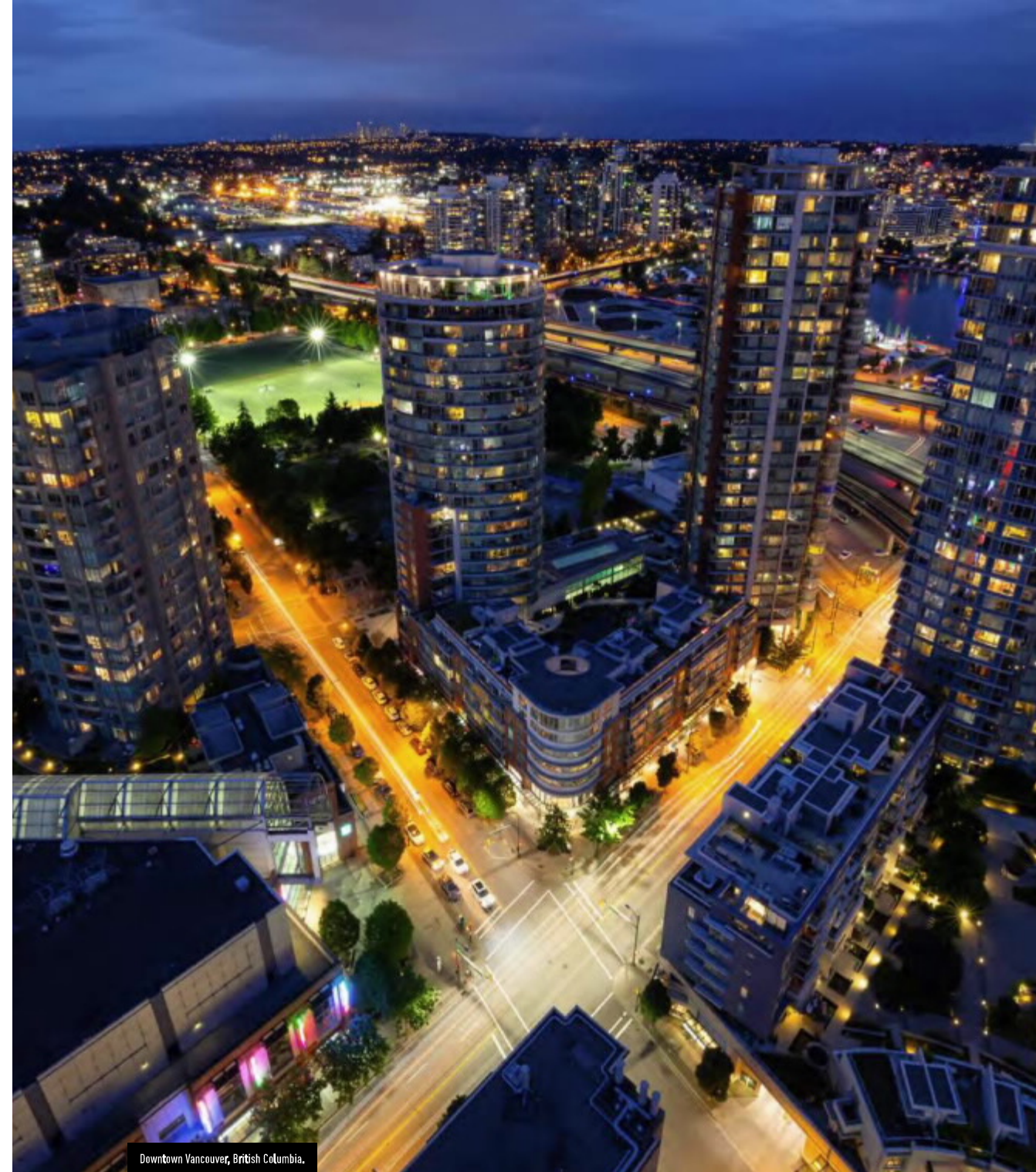
Anti 2SLGBTQIA+ and antisemitic rhetoric is spreading widely through social media and online forums among domestic RMVE adherents, increasing the risk of extremist violence against these communities, and placing youth vulnerable to RMVE propaganda at a higher risk of becoming radicalized on online platforms. 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 advice.

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 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,

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.



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. ■



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



Grands-Jardins National Park, Charlevoix, Quebec.

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.

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. Akeagok, 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. ■



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

The Evolution of Disinformation: A DEEPAKE FUTURE



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

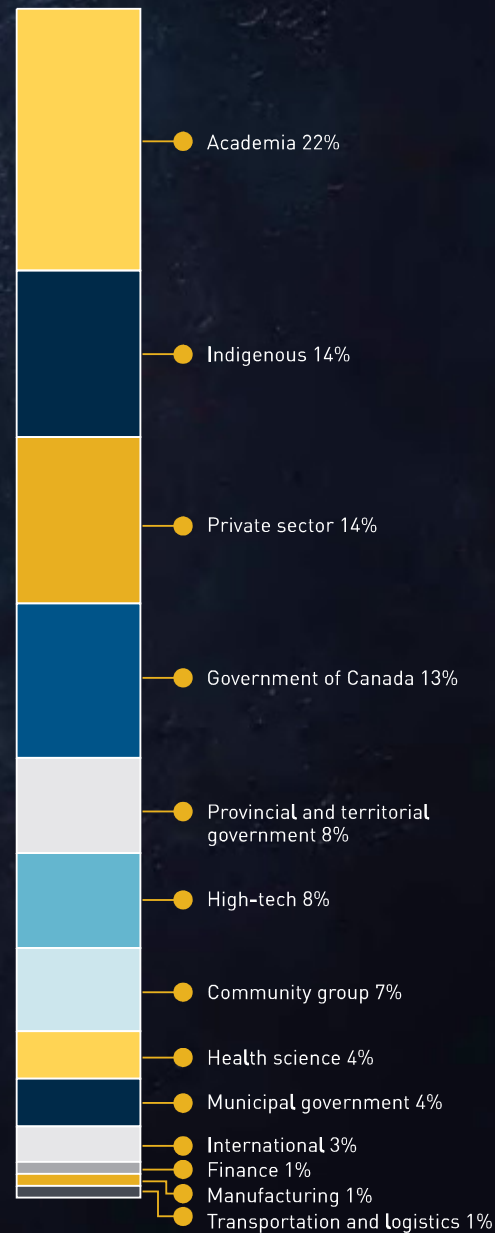
Indigenous groups. In March, CSIS presented at the Inuit Technology Forum in Iqaluit. The presentation, made available in Inuktitut to the participants, focused on cyber threats to the security of Canada. In November, CSIS, Inuit Tapiriit Kanatami, and the Privy Council Office established a mechanism 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. ■

Percentage of CSIS Engagements by Sector



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:

	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

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.

C SIS 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.

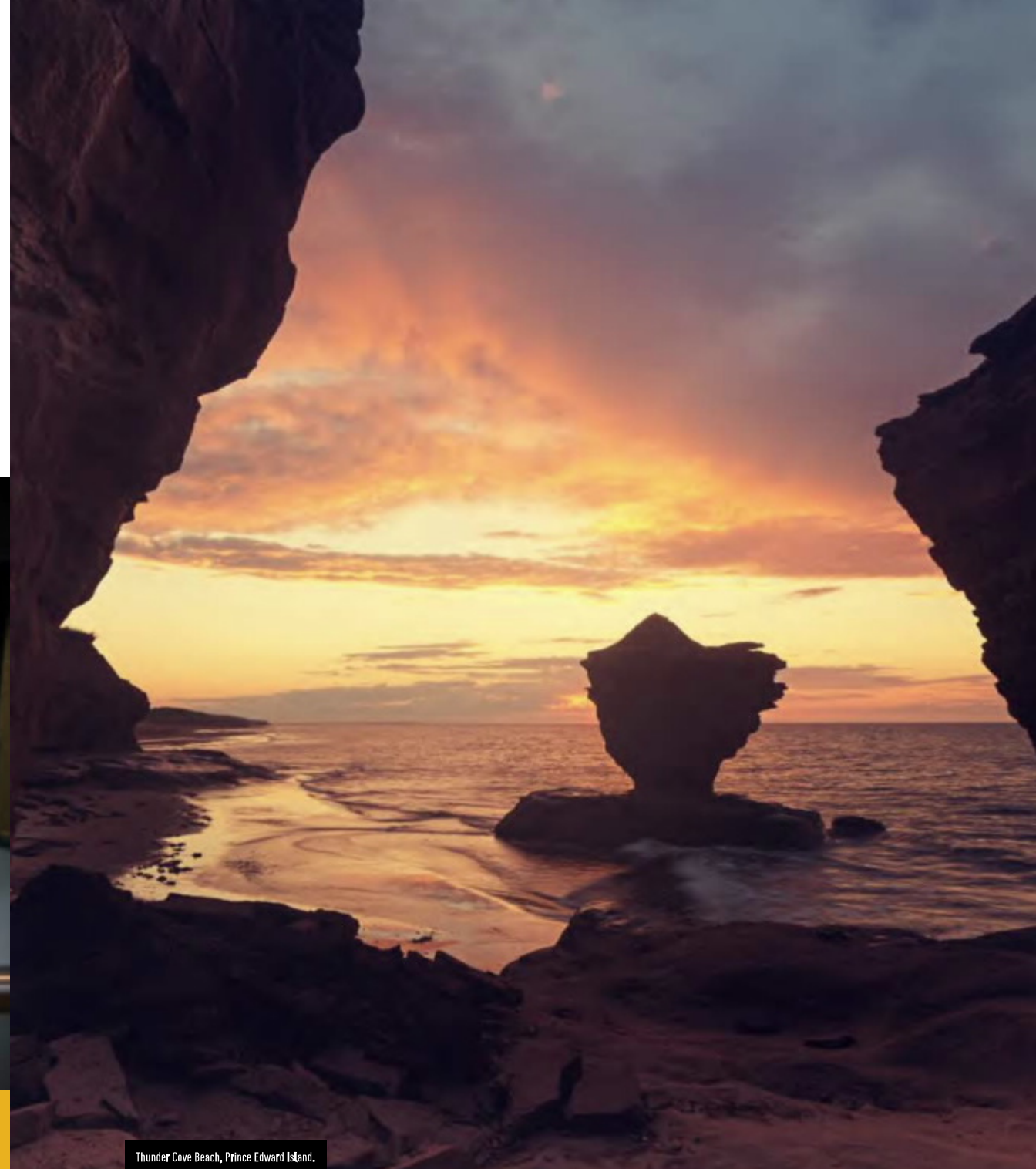
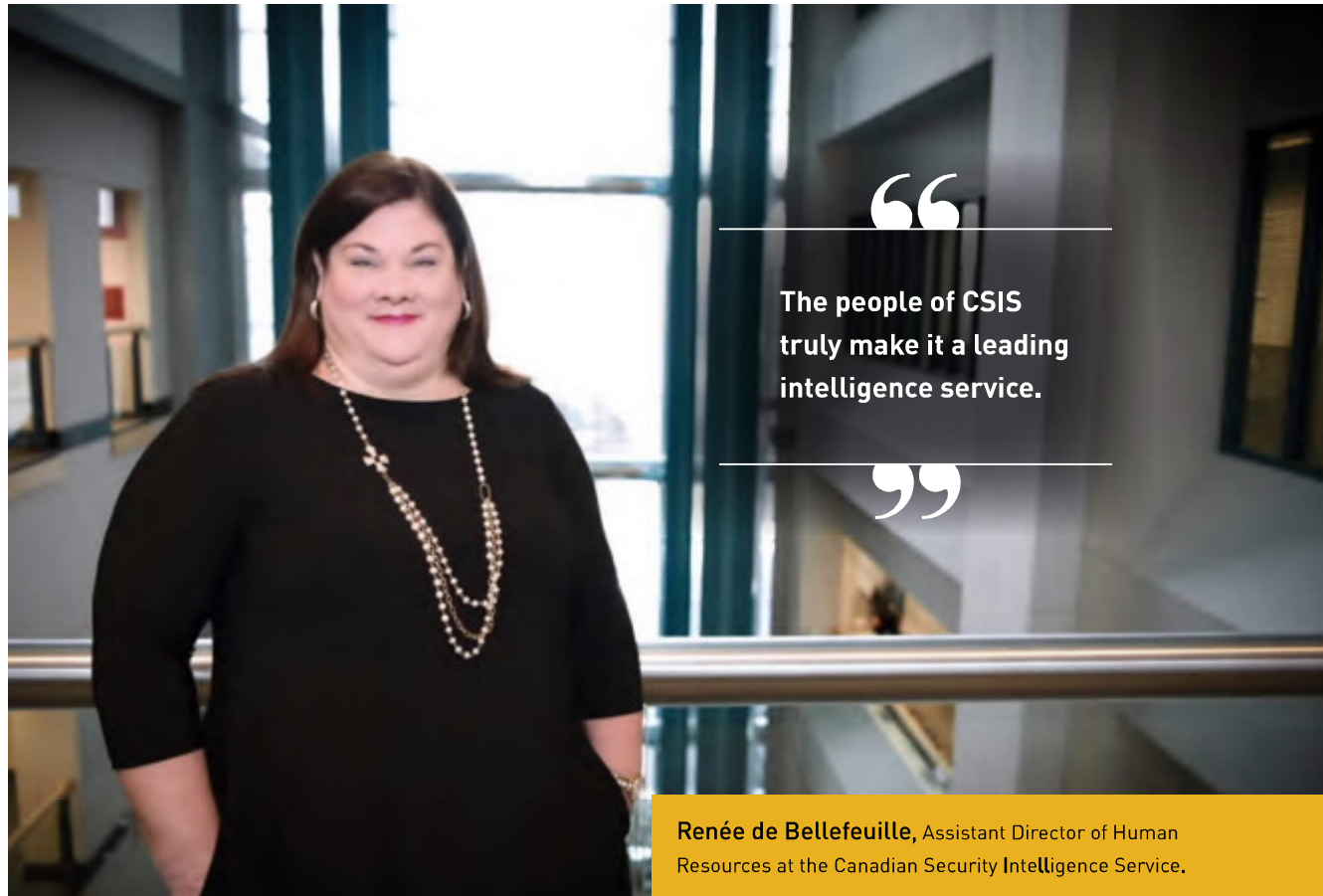
In recent years, CSIS has made great strides in ensuring that its workforce is representative of Canadian society. Not only is this the fair and right objective, but it also ensures CSIS is operationally better as it can draw on the cultural, linguistic, and personal experiences of employees from across 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. ■



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,

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.

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.

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	\$259,284,441	\$238,065,778	\$256,628,559

*Salary costs include Employee Benefits Payments

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



“

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.

”

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

intelligence partners, who may begin to doubt our ability to protect not only our own secrets, but theirs as well.

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>