



Communications  
Security Establishment

Centre de la sécurité  
des télécommunications

ISSN 2564-047X  
CAT D95-11E-PDF

Communications  
Security Establishment  
**ANNUAL  
REPORT**  
2022-2023

Communications Security Establishment  
1929 Ogilvie Road,  
Ottawa, ON K1J 8K6  
[cse-cst.gc.ca](http://cse-cst.gc.ca)

ISSN 2564-047X  
CAT D95-11E-PDF

© His Majesty the King in Right of Canada, as represented  
by the Minister of National Defence, 2023

# Table of contents

CSE at a glance	2
Foreword from the Minister of National Defence	3
Message from the Chief	4
Foreign signals intelligence	7
Foreign cyber operations	8
International partners	9
Russia's invasion of Ukraine	10
Foreign interference and threats to democracy	12
Countering hostile state activity	15
Countering terrorism and extremism	17
Cybercrime	17
Requests for technical and operational assistance	19
Economic security	19
Communications Security	21
Cyber security	23
Promoting digital resilience for Canadians	31
Innovation	38
Accountability	43
People	51
Endnotes	61

## CSE at a glance

The Communications Security Establishment (CSE) is Canada's foreign signals intelligence agency, and technical authority for cyber security and information assurance.

CSE includes the [Canadian Centre for Cyber Security](#)<sup>1</sup> (Cyber Centre), which is the federal government's operational lead for cyber security.

CSE's mandate is detailed in the [Communications Security Establishment Act](#)<sup>2</sup> (*CSE Act*) and has 5 parts:

- foreign intelligence
- cyber security
- active cyber operations
- defensive cyber operations
- technical and operational assistance to federal partners

The Chief of CSE, Caroline Xavier, was appointed on August 30, 2022.

The Chief reports to the Minister of National Defence, the Honourable Anita Anand.

CSE's 2022 to 2023 total authorities were \$948 million.

Our workforce is 3,232 full-time, permanent employees.

This report is an unclassified summary of CSE's activities from April 1, 2022 to March 31, 2023.

Unless otherwise specified, "this year" refers to the fiscal year.

## Foreword from the Minister of National Defence



In November 2022, I gave the keynote speech at Big Dig, the classified, cyber security workshop held every year at CSE. What I saw gave me hope: experts from across the Government of Canada, plus international allies and tech industry partners, working together on some of the hardest cyber security challenges Canada faces.

These challenges can have very serious consequences. As cyber threat actors have increased their activity, CSE has issued numerous warnings to Canadian critical infrastructure providers. These are wake-up calls for us all.

As this report shows, CSE and its Canadian Centre for Cyber Security are working hard to defend Canada from a wide variety of threats to our national security, our economic security and even our democracy itself. We must be clear-eyed about the threats we face, and we must work with all stakeholders, including partners around the world to defend our common interests.

As part of the defence portfolio, CSE has continued to play a key role in supporting Canada's response to Russia's invasion of Ukraine. This has included exposing Russia's ongoing disinformation efforts and providing cyber security support to Ukraine and Latvia.

Going forward, CSE will play an important role in Canada's Indo-Pacific strategy. Launched in November 2022, the strategy includes a multi-department project to help Canada's partners in the Indo-Pacific region develop their cyber security capacity.

CSE is filled with hard-working and dedicated public servants as I witnessed that day at Big Dig. As Defence Minister I know that this event is just a sliver of the work that goes on at CSE every day to protect Canada and Canadians. For the achievements outlined in this report, and for those that must remain secret, CSE has my deepest respect and sincerest thanks.

- The Honourable Anita Anand,  
Minister of National Defence

## Message from the Chief

It's an honour to be able to share this report with Canadians as the new Chief of CSE. In my short time as Chief, I am very proud of what CSE has accomplished this past fiscal year.

CSE's mandate includes countering some of the toughest national security challenges we face, from hostile state activity like foreign interference to cybercrime. I hope this report gives readers a sense of the diligence, skill and constant innovation that go into countering those threats.

For more information on the threats themselves, I highly recommend the Cyber Centre's [National Cyber Threat Assessment 2023-2024](#).<sup>3</sup> Published this past October, it is a sobering read, but an essential one.

In light of these growing threats, [Budget 2022](#)<sup>4</sup> allocated funds to expand CSE's capacity. We are in growth mode. This means trying new things, like bringing in candidates at different security levels and offering telework options outside the National Capital Region.

If you know a Canadian who is looking for a career that truly matters, send them our new [recruitment video](#).<sup>5</sup> We are hiring for all sorts of roles.

Growth also gives CSE a prime opportunity to diversify our workforce. Since starting my role in August, I've been delighted to see evidence all around me of CSE's commitment to equity, diversity and inclusion (EDI). The People chapter contains some significant milestones, including:

- the official launch of our EDI framework
- CSE's first Accessibility Plan
- CSE's first sponsorship pilot program for Black, Indigenous and racialized employees

As always, there are parts of our work that we cannot share in a public report. We don't identify specific targets of our signals intelligence gathering or foreign cyber operations. These are classified. However, we do give examples of some of the intelligence priorities CSE supports.

For example, this report dedicates a chapter to foreign interference and democracy. Instead of separating CSE's efforts by mandate type, we bring them together in one place. Besides being easier for the reader, this is also more reflective of how CSE operates in general.

## Message from the Chief

---

Our cyber security activities are informed by foreign signals intelligence and vice versa. Our foreign cyber operations capabilities enable us to act on the threats we identify through the other parts of our mandate.

Because CSE is limited in what we can say publicly, we place great value on the external oversight and review bodies who scrutinize our work on behalf of Canadians. For example, the section on metadata sharing outlines how closely CSE worked with the Office of the Privacy Commissioner before implementing a new process for sharing certain types of metadata with our closest allies. We have worked with the National Security and Intelligence Review Agency (NSIRA) to give them independent access to CSE files related to NSIRA reviews.

Likewise, CSE welcomes the independent reviews launched in March 2023 to examine foreign interference in Canada's elections. We will support them in any way we can.

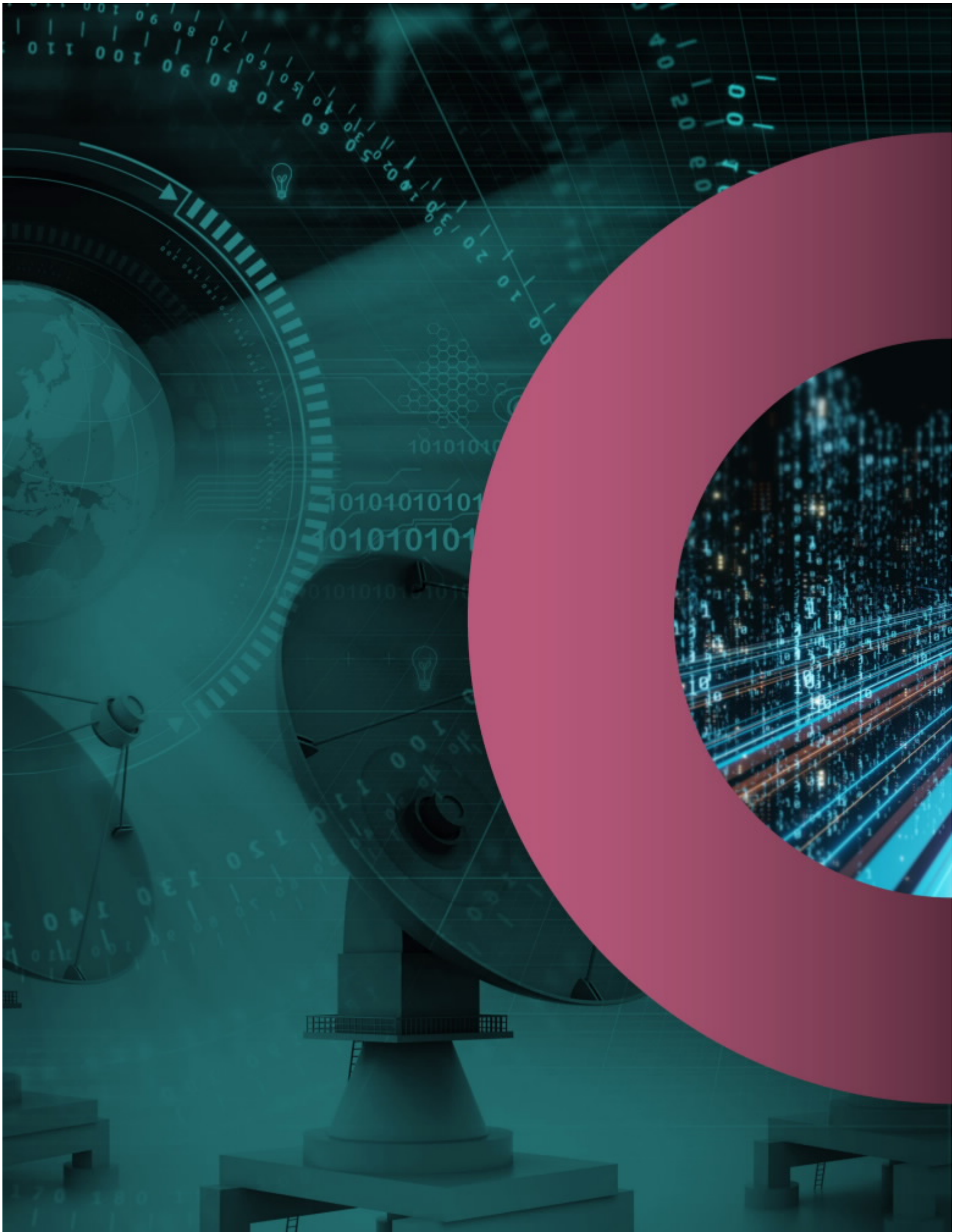
The threats we face are real. Canadians need to know they can trust Canada's security and intelligence community to counter them effectively, lawfully **and** ethically.

I am grateful to my predecessors, especially Chief #10, Shelly Bruce, for building an organization worthy of that trust.

It's my honour and pleasure to take the lead for the next leg of the journey.

- Caroline Xavier  
she/her  
Chief, CSE #11







## Foreign signals intelligence

CSE is Canada's foreign signals intelligence (SIGINT) agency. That means we intercept and analyze foreign electronic communications to provide the Government of Canada with unique information about foreign threats to Canadian security and prosperity and important insights to support foreign policy and decision making. We are forbidden by law from targeting the communications of Canadians or anyone in Canada.

CSE's foreign signals intelligence collection is guided by the Government of Canada's intelligence priorities established by Cabinet. Foreign intelligence reports are disseminated to clients across government and also shared with key foreign partners.

This fiscal year, CSE produced and disseminated classified reports on a range of Government of Canada priorities including:

- Russia's invasion of Ukraine
- foreign interference, malign influence and disinformation
- other hostile state activity such as:
  - espionage
  - sabotage
  - intellectual property theft
- Arctic sovereignty
- instability in Haiti
- cybercrime
- cyber threat intelligence
- terrorism and extremism
- supporting the Canadian Forces during its air, sea, land and special forces overseas operations globally
- threats to Canadians abroad

CSE foreign intelligence directly supports other aspects of CSE's mandate including:

- cyber security for federal institutions, including Crown corporations, and critical infrastructure
- foreign cyber operations

### CSE foreign intelligence reporting 2022 to 2023



## Working with the Canadian Armed Forces

CSE works in close collaboration with the Canadian Armed Forces (CAF) to integrate, prioritize and deconflict military signals intelligence operations in support of defence intelligence requirements.

This partnership ensures that CAF has improved domain awareness and force protection as it conducts its operations globally.

Together we continue to partner operationally and strategically at every level to align our strategic outcomes and maximize Canada's strategic advantage in international affairs, defence, security and cyber security.

This year CSE worked very closely with CAF partners to provide intelligence:

- in support of NORAD
- on the Russian invasion of Ukraine
- on Arctic sovereignty
- in support of military operations IMPACT, REASSURANCE and UNIFIER



## Foreign cyber operations

CSE's mandate includes taking action online to counter foreign-based threats and advance Canada's international affairs, defence, or security interests.

These foreign cyber operations (FCO) can be either:

- defensive: to protect the Government of Canada or systems of importance from malicious cyber activity; or
- active: to disrupt foreign adversaries

In 2022, the Minister of National Defence issued 4 Ministerial Authorizations for FCO:

- 1 for defensive cyber operations (DCO)
- 3 for active cyber operations (ACO)

For more information on how foreign cyber operations are authorized, see the [Accountability](#) section (p.43).

CSE's foreign cyber operations are informed by both our foreign intelligence mandate **and** our cyber defence capabilities.

Since the *CSE Act* came into effect in 2019, CSE has conducted active cyber operations to:

- counter hostile state activity
- counter cybercrime
- disrupt foreign extremists
- assist the Canadian Armed Forces

Budget 2022 announced funds to bolster CSE's ability to conduct foreign cyber operations. On a cash basis, this funding amounts to:

- \$273.7 million over 5 years, starting in 2022 to 2023, and \$96.5 million ongoing<sup>6</sup>

This will enable CSE to better defend Canada's government and critical infrastructure systems from cybercrime, as well as state-sponsored cyber activity.

## Responsible behaviour in cyberspace

Canada supports the rules-based international order, which includes behaving responsibly in cyberspace.

Under the *CSE Act*, foreign cyber operations must not:

- be directed at Canadians or anyone in Canada
- cause death or bodily harm
- interfere with the course of justice or democracy

CSE consults extensively with federal partners including Global Affairs Canada and the Department of Justice to ensure that proposed foreign cyber operations are in line with:

- Canadian legal requirements
- Canada's obligations under [international law applicable in cyberspace](#)<sup>7</sup>
- voluntary norms of acceptable State behaviour in cyberspace
- Canada's foreign policy objectives

The Minister of Foreign Affairs must consent to active cyber operations and must be consulted on defensive cyber operations.

In addition, all our operations are subject to external review to ensure they comply with our mandate and legal responsibilities.

Working within these requirements, CSE is able to counter threats to Canada and Canadians while reinforcing appropriate state behaviour in cyberspace.

## International partners

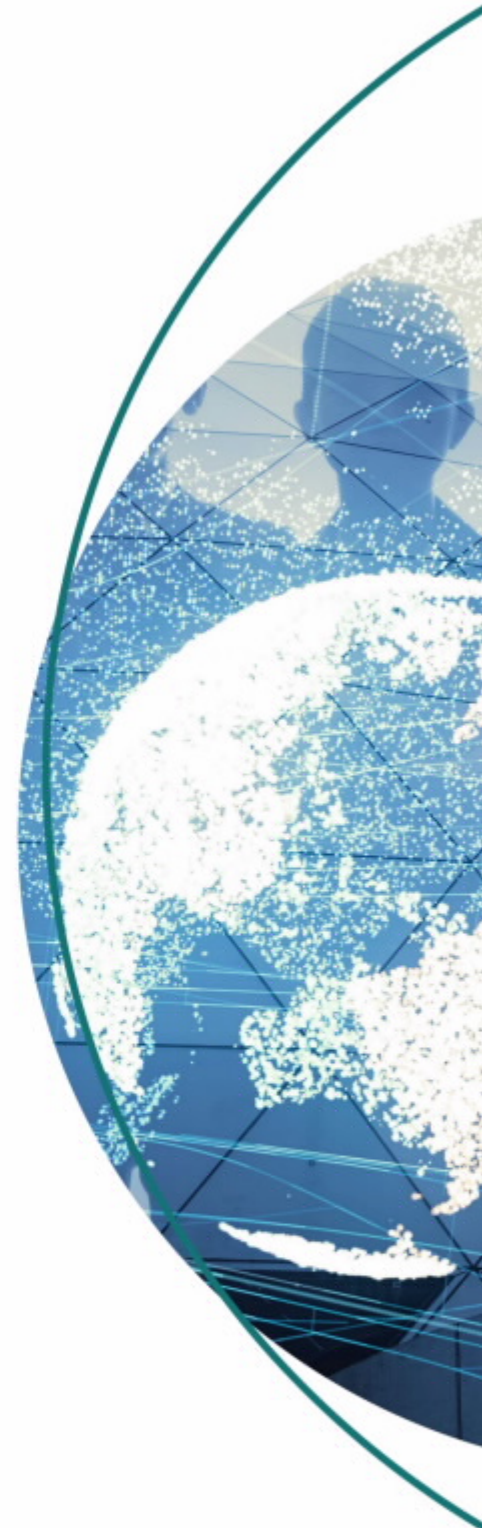
CSE works with signals intelligence and cyber defence counterparts around the world to promote our common security.

Our closest intelligence-sharing relationships are with the other Five Eyes countries: the United States, the United Kingdom, Australia and New Zealand.

This year, CSE continued to work hand in hand with our Five Eyes allies to protect our shared national interests and to keep Canadians safe. We continued to deliver relevant and timely intelligence to this community and to leverage the shared expertise of the Five Eyes to satisfy Canada's foreign intelligence requirements.

In January 2023, CSE resumed sharing metadata with our Five Eyes partners. The Accountability chapter outlines the steps CSE took to address privacy concerns before sharing resumed (see [Metadata sharing](#) on p.46).

It is important to note that CSE does not ask our Five Eyes partners to do anything on our behalf that is not legal for us to do (such as target the communications of Canadians or anyone in Canada).



## Russia's invasion of Ukraine

Since Russia's invasion of Ukraine in February 2022, Canada has steadfastly supported the Ukrainian people as they fight for their sovereignty.

CSE has worked closely with domestic partners and international allies to support a unified global response. Our activities have included:

- providing the Government of Canada with actionable signals intelligence to:
  - support Canadian and allied policy responses (such as sanctions)
  - monitor for malicious Russian cyber activity against Canada, Ukraine and NATO allies
  - protect Canadian diplomatic personnel, government delegations and military members in Ukraine
- providing signals intelligence and cyber security support to Operation UNIFIER, the Canadian Armed Forces training mission in support of Ukraine
- working closely with our allies to address high-priority intelligence needs
- bolstering the Government of Canada's defences against known Russian-backed cyber threat activity
- countering Russian disinformation
- sharing cyber threat information with:
  - key partners in Ukraine
  - NATO allies
  - Canadian critical infrastructure

These activities have continued this fiscal year.

### Countering Russian disinformation

CSE's intelligence indicates that Kremlin officials have guided and coordinated campaigns to spread disinformation about the invasion. This included false stories accusing Canadian forces of committing war crimes in Ukraine and accusing the United States of using Ukraine as a biological testing ground.

In April 2022, CSE shared these and other examples of Russia-backed disinformation with Canadians (summarized in the [CSE Annual Report 2021-2022](#)<sup>8</sup>). This was the first time CSE has ever posted declassified intelligence on social [media](#).<sup>9</sup>

In July 2022, CSE used social media again to expose further **false** claims by Russia that:

- "Ukrainian radicals" had sabotaged chemical and nuclear sites in Ukraine
- the "sabotage" was part of a plan to accuse Russia of using chemical and nuclear weapons against Ukrainian civilians
- "Ukrainian neo-Nazis" possessed chemical weapons that could be used against civilians

Each time, CSE also shared guidance to help Canadians identify and take action against disinformation. As of March 2023, these social media posts had been seen over 650,000 times.



## Cyber assistance to Ukraine and Latvia

On March 17, 2022, the Minister of National Defence signed 2 Ministerial Orders designating the electronic information and networks of Ukraine and Latvia as systems of importance (SOIs) to the Government of Canada.

This was the first time a Minister has used their powers under the *CSE Act* to designate entities **outside Canada** as SOIs.

The designations allow CSE to provide cyber security assistance to help protect the designated entities.

The orders are still in effect and CSE's assistance is ongoing.

### Assistance to Ukraine

Over the past year, the Cyber Centre has notified Ukraine about:

- hostile cyber activities against Ukraine's national infrastructure
- vulnerabilities on their network infrastructure to prevent hostile activity

This work is based on data shared proactively with CSE by the Ukrainian authorities.

In October 2022, the Minister of National Defence announced approximately \$2 million in funding to provide satellite communications services for Ukraine. This joint project between the Canadian Armed Forces and Department of National Defence (CAF/DND), CSE, and the satellite operator, Telesat, came into effect on April 1, 2023, and will help Ukraine maintain continuity of services, including critical cyber systems.

We are working with our Ukrainian counterparts to identify areas where CSE could provide additional cyber assistance.

### Deployments to Latvia

At the request of our Latvian allies, the Cyber Centre has deployed personnel to help defend against cyber threats on Latvia's critical infrastructure and government networks.

These deployments are part of a joint mission involving cyber security experts from the Department of National Defence, the Canadian Armed Forces, the Cyber Centre and its Latvian counterpart, CERT.LV.

Over the course of 4 deployments this fiscal year, Cyber Centre personnel have helped to defend Latvia's cyberspace by:

- investigating cyber incidents
- carrying out cyber threat hunting operations
- identifying adversarial threat activity on critical networks
- providing on-site tools and training
- making recommendations
- sharing best practices
- improving cyber security coordination between Canada and our NATO allies

This joint mission has helped to defend NATO's eastern flank from adversarial cyber threats. Cyber Centre deployments to Latvia are ongoing in fiscal year 2023 to 2024.

**It's pretty daunting deploying on a mission like this. But once we got there, we realized, 'We belong here. We have the expertise to really make a difference'.**

JD, Cyber Centre analyst

## Public information sharing

This year, the Cyber Centre issued the following public reports, alerts and guidance documents related to Russian-backed cyber threats:

- [Joint cyber security advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure](#)<sup>10</sup> (April 2022)
- [Cyber threat activity related to the Russian invasion of Ukraine](#)<sup>11</sup> (July 2022)
- [Cyber security for heightened threat levels](#)<sup>12</sup> (July 2022)
- [Risk of malicious cyber activity against Ukraine-aligned nations](#)<sup>13</sup> (February 2023)

The Cyber Centre issued 3 other joint cyber security advisories with Five Eyes partners to warn about cyber techniques associated with Russian-backed actors.

In addition, the Cyber Centre held briefings for Canadian critical infrastructure organizations including the Provinces and Territories on the increased risk of cyber threat activity.

## Foreign interference and threats to democracy

Hostile state actors are attempting to influence and interfere with Canada's society and democracy in various ways, including espionage, malicious cyber activity and online disinformation.

Countering this activity requires a whole of government approach, which CSE actively supports by:

- providing foreign signals intelligence to Government of Canada decision makers about the intentions, capabilities and activities of foreign-based threat actors
- defending Canada's federal elections infrastructure from malicious cyber activity
- proactively helping democratic institutions improve their cyber security
- sharing unclassified threat assessments with the public
- sharing information to help Canadians:
  - identify disinformation
  - protect their privacy and security online

## SITE Task Force

Since 2019, CSE has served on the [Security and Intelligence Threats to Elections \(SITE\) Task Force](#),<sup>14</sup> along with CSIS, the RCMP and Global Affairs Canada. CSE's role is to monitor foreign signals intelligence and cyber activity on Government of Canada networks for signs of foreign interference in the electoral process.

Throughout the election period, SITE partners brief a panel of senior public officials under Canada's [Critical Election Incident Public Protocol](#).<sup>15</sup> This panel decides whether the activities reported to them affect Canada's ability to have a free and fair election. If that threshold is met, there is a set protocol for informing the public.

During both the 2019 and 2021 federal elections the panel reported that, while attempts at foreign interference did take place, the elections were still free and fair.

In March 2023, the Prime Minister announced new measures to [strengthen confidence in Canada's democracy](#).<sup>16</sup> This included requesting external reviews of the 2019 and 2021 elections to assess what foreign influence took place and how national security agencies, including CSE, responded to the threat.

CSE continues to cooperate fully with these reviews to build trust in Canada's election process and to strengthen it against foreign interference.

The SITE Task Force continued to meet regularly throughout the past year to:

- remain connected as a community
- continue to monitor ongoing foreign interference activities

## Defending elections infrastructure

CSE's mandate includes conducting defensive cyber operations (DCO) to respond to cyber attacks on critical systems.

In the run-up to both the 2019 and 2021 federal elections, the Minister of National Defence issued an authorization for DCO which included protecting the electronic infrastructure of Elections Canada. This was a precaution in case of malicious cyber activity during the election period. For example, if a foreign threat actor had compromised Elections Canada's website, CSE could have used our cyber operations capabilities to impact the server being used for the attack. In the event, no activities took place that would have required a DCO response. However, DCO are an important tool for countering cyber threats to Canada's democratic processes.





## Cyber security for democratic institutions

Democratic institutions are an essential part of Canada's critical infrastructure. The Cyber Centre works with elections authorities and federal political parties to help them strengthen their cyber security.

In the run-up to both the 2019 and 2021 federal elections, the Cyber Centre worked with federal political parties to brief them on cyber threats and advise them on cyber security best practices. In both cases, the Cyber Centre set up a 24/7 hotline that candidates could call if they had any cyber security concerns. Outside election periods, the Cyber Centre has a dedicated point of contact political parties can reach out to on cyber security matters.

In March 2022, the Cyber Centre updated parties on the increased risk of Russian-backed cyber threat activity following the invasion of Ukraine. Representatives from 5 parties attended the briefing, which included cyber security recommendations. The Cyber Centre sent the content of the briefing to all 19 registered federal political parties.

This fiscal year the Cyber Centre:

- supported elections authorities ahead of provincial elections in Quebec, Ontario and Alberta
- shared guidance resources with municipalities
- provided elections authorities with:
  - briefings on the National Cyber Threat Assessment
  - technical advice
  - guidance resources
  - cyber security services

## Cyber security for voting technologies

Since 2022, the Cyber Centre has been contributing to the development of the first ever technical standards for election and voting technologies in Canada. Cyber Centre experts are participating in technical committees to help develop standards for:

- online voting in Canadian municipal elections
- vote tabulators
- electronic poll books

The process is being led by the Digital Governance Standards Institute, which released the [first draft standards](#)<sup>17</sup> for public review in April 2023.

## Information on cyber threats to elections

In May 2022, CSE created a dedicated web page on [cyber threats to elections](#).<sup>18</sup> The page provides an overview of ways in which threat actors can disrupt democratic processes, such as:

- disrupting election infrastructure using distributed denial of service (DDoS) attacks
- mimicking user identities to spread false information on social media
- compromising political parties' IT systems
- launching online foreign influence campaigns to discredit the democratic process
- using ransomware to disrupt access to election data

The web page contains links to Cyber Centre reporting on cyber threats to Canada's democratic process. It also provides up to date cyber security advice and guidance resources for:

- political parties
- elections authorities
- voters



## Disinformation and democracy

Disinformation is false information that is deliberately created to cause harm. Often designed to provoke an emotional response, disinformation spreads very quickly on social media. This makes it harder for Canadians to know what is true or who to trust.

Foreign states use online disinformation to destabilize Canada's democracy by:

- spreading false information
- influencing voter decisions
- polarizing opinions
- discrediting people and institutions
- undermining trust in the democratic process

This year, CSE contributed to a government-wide [online disinformation](#)<sup>18</sup> awareness campaign. The campaign includes:

- tools to help Canadians identify and fact-check disinformation
- content and videos from external partners like MediaSmarts and CIVIX: CTRL-F
- information from Cyber Centre threat reports including:
  - the [National Cyber Threat Assessment](#)<sup>20</sup>
  - [Cyber threats to Canada's democratic process \(July 2021 update\)](#)<sup>21</sup>
- Cyber Centre guidance on [how to identify misinformation, disinformation and malinformation](#)<sup>22</sup>



## Countering hostile state activity

CSE leverages all aspects of our mandate (foreign intelligence, cyber security, foreign cyber operations and technical and operational assistance) to counter hostile state activities. These threats include espionage, malicious cyber activity and foreign interference.

### Public attributions

Canada supports and advocates for responsible state behaviour in cyberspace.

In April 2022, Global Affairs Canada set out Canada's position on [International Law applicable in cyberspace](#).<sup>23</sup> Global Affairs Canada works with international allies to call out state behaviour that violates these norms.

This fiscal year, CSE intelligence reporting and cyber security analysis contributed to public attributions of:

- [Russia's malicious cyber activity affecting Europe and Ukraine](#)<sup>24</sup> (May 2022)
- [Iran's malicious cyber activity affecting Albania](#)<sup>25</sup> (September 2022)

## Countering hostile state activity

### State-backed cyber actors

CSE leverages its foreign intelligence, defensive and active cyber operations, and cyber defence mandate to counter foreign cyber actors, including state-backed actors.

State-backed cyber actors pose the greatest strategic threat to Canada and Canada's critical infrastructure. These adversaries use highly sophisticated and covert techniques against Canada and allied countries with ambitions ranging from intelligence collection to destructive acts.

CSE signals intelligence continues to provide unique and timely insight into the tactics, techniques and procedures used by a broad spectrum of state-backed cyber actors. This in turn informs the advice and guidance generated by the Cyber Centre.

As these and other cyber threats continue to evolve, cyber defence informed by intelligence will provide a strategic advantage for Canada.

### Transnational repression

Authoritarian states use a variety of means to monitor and intimidate diaspora populations around the world, including in Canada. An example of this is the issue of the People's Republic of China operating "police service stations" in Canada.

CSE works with global and federal partners to mitigate the risks posed by these transnational repression activities. We do this by gathering foreign signals intelligence and by supporting Canada's security and intelligence community.

### High-altitude surveillance balloon

In January and February 2023, a high-altitude surveillance balloon belonging to the People's Republic of China violated Canadian and US airspace before being safely shot down by the US Air Force.

CSE remained in close contact with our US counterparts throughout the situation. We worked closely with domestic partners including the Canadian Armed Forces (CAF) to support the Canadian government's response and to ensure Canada and Canadians remained safe.

### Arctic sovereignty

CSE works to make sure the Government of Canada has the necessary intelligence to safeguard Canada's Arctic sovereignty.

Working closely with the CAF, CSE seeks to ensure Canada can predict, defend and deter adversaries that seek to exploit this region and threaten Canadian interests there. This includes monitoring and understanding the intentions, capabilities and investments of hostile state actors with respect to the Arctic.

CSE chairs a multi-national signals intelligence forum which focuses on the Polar regions. We collaborate and coordinate with partners across the Government of Canada to ensure that our intelligence gathering efforts align with their needs.

**There is growing international interest and competition in the Canadian Arctic from state and non-state actors who seek to share in the region's rich natural resources and strategic position...[This] brings safety and security challenges to which Canada must be ready to respond.**

[Canada's Arctic and Northern Policy Framework](#)<sup>26</sup>

## Countering terrorism and extremism

CSE, under its foreign intelligence mandate, works to identify foreign terrorist and extremist threats directed towards Canada and its allies. These threats include:

- Religiously Motivated Violent Extremism (RMVE)
- Ideologically Motivated Violent Extremism (IMVE)

This year, CSE was able to provide both domestic and allied partners with unique intelligence on the networks, capabilities, motivations and intentions behind extremist activities.

Additionally, CSE generated intelligence to support foreign cyber operations and the disruption of extremist activities.

For example, CSE conducted active cyber operations to disrupt and remove harmful terrorist content disseminated online by foreign, ideologically-motivated extremists. This disruption fractured the extremists' group cohesion and significantly reduced their online reach and ability to recruit new members.

Due to the complex nature of extremist networks and the breadth of extremist topics, CSE works closely with partners to provide intelligence to support the disruption of extremist activities. In this vein, CSE continued to participate in a multi-national signals intelligence forum which focuses on counterterrorism and facilitates signals intelligence collaboration across partners. As part of this community CSE is better placed to protect Canadians and Canadian interests.

## Cybercrime

Cybercrime is big business for the cybercriminals and has major impacts on Canada's economic security. As we outlined in the National Cyber Threat Assessment, the average ransomware payment in 2022 was over \$250,000 CAD. This does not include other costs including:

- service disruptions
- identity theft
- intellectual property theft
- IT recovery costs
- reputational damage

**Cybercrime continues to be the cyber threat activity most likely to affect Canadians and Canadian organizations.**

[National Cyber Threat Assessment 2023-2024<sup>27</sup>](#)

## Understanding cybercrime

CSE conducts in-depth research into the cybercrime ecosystem. These assessments draw on:

- classified intelligence
- incidents reported to the Cyber Centre
- commercial data
- publicly available information such as news articles

This year, the Cyber Centre assessed the main ransomware groups affecting Canada to create a series of threat ranking reports. The reports contain actionable information on the characteristics of each group to help cyber defenders prioritize their resources.

The Cyber Centre shared the threat ranking with federal and Five Eyes partners to help guide coordinated actions to counter these threats. We are preparing a version to be shared with critical infrastructure clients in the new fiscal year.

Assessments like the threat ranking report also help CSE and the Cyber Centre to plan our own activities. This includes both cyber security, and active cyber operations.

## Countering cybercrime

CSE uses the breadth of its mandate to reduce the impact of cybercrime on Canadian businesses, organizations and individuals. Ongoing efforts include:

- collecting intelligence on cybercrime groups
- enhancing our cyber defences to protect critical systems against cybercrime threats
- advising Canadian critical infrastructure providers on how to protect themselves against cybercrime
- using our active cyber operations capabilities (ACO) to disrupt the activities of cybercrime groups

For example, under these authorities, CSE has launched an enduring campaign to disrupt foreign cybercriminals who threaten Canadian and allied systems with ransomware attacks. These systems include health care providers and other critical infrastructure owners.

Under this campaign, CSE has executed dozens of operations that have disrupted the foreign infrastructure used by these groups. These operations have allowed the Cyber Centre and other cyber defenders to work with these system owners to prevent them from becoming victims of ransomware attacks.

In addition, working with Canadian and allied partners, CSE has conducted ACO to reduce the ability of cybercrime groups to:

- target Canadians, Canadian businesses and institutions
- launch ransomware attacks
- solicit, buy and sell cybercrime goods and services including:
  - Canadian personal information
  - Canadian proprietary information
  - malware

These operations imposed costs on cybercrime groups by making their activities more difficult and less profitable. The aim is to deter future cybercrime attempts on Canadian targets.

## Requests for technical and operational assistance

## Requests for technical and operational assistance

Under the *CSE Act*, federal law enforcement, defence and national security partners may request technical and operational assistance from CSE. This saves the government from replicating costly capabilities and expertise across multiple departments including:

- Royal Canadian Mounted Police (RCMP)
- Canadian Security Intelligence Service (CSIS)
- Canada Border Services Agency (CBSA)
- Canadian Armed Forces and the Department of National Defence (CAF/DND)

In these cases, CSE operates under the authorities of the requesting partner.

CSE, RCMP and CSIS meet regularly as part of the Technical Partnerships Steering Committee (TPSC) to drive deeper collaboration between the agencies, leveraging the strengths and capabilities of each agency to fulfill our independent mandates, with a view to reducing duplication of effort as much as possible.

In 2022, CSE received 62 requests for technical and operational assistance from federal partners. Of these, 59 were approved, 1 was denied and 2 were cancelled.

The number of requests for technical and operational assistance over the last 3 years was as follows:

- 2022:
  - Received: 62
  - Approved: 59
- 2021:
  - Received: 35
  - Approved: 32
- 2020:
  - Received: 24
  - Approved: 23

## Economic security

CSE is one of many federal departments and agencies that work to safeguard Canada's economic security. To do this we leverage our foreign intelligence mandate, our cyber security mandate and our technological expertise.

### Safeguarding research

Canada's future prosperity depends on Canadian research and intellectual property. Both are frequent targets of cyber espionage. CSE helps protect Canada's economic security by advising Canadian research organizations on how to protect their valuable information.

In some cases, protecting that information is also a matter of national security.

In July 2021, Innovation, Science and Economic Development Canada released new [National Security Guidelines for Research Partnerships](#).<sup>28</sup> These guidelines aim to safeguard Canadian scientific research from ending up in the hands of actors who pose a threat to Canada's national security, such as foreign governments or militaries.

In July 2022, CSE and other national security partners began the national security risk review process under these guidelines.

**State-sponsored threat actors engage in commercial espionage, targeting intellectual property and other valuable business information with the goal of sharing stolen information with state-owned enterprises or domestic industry in their home country.**

[National Cyber Threat Assessment 2023-2024](#)<sup>29</sup>

## Economic security

### National security assessments

CSE also continued to provide national security assessments to government partners in support of:

- the *Investment Canada Act*
- the *Export and Import Permits Act*

In addition, CSE assisted the Bank of Canada and the Department of Finance to design national security safeguards in support of the *Retail Payment Activities Act*, which received royal assent in June 2021.



### Supply chain integrity

When government departments procure IT products, they must make sure those products will keep data and communications secure. Vulnerabilities can occur at any stage of the product lifecycle from design to deployment to maintenance. These are known as supply chain risks.

This year, the Cyber Centre conducted over 1300 supply chain integrity risk assessments for government clients. Considerations include:

- Does the technology meet international standards?
- Who is the vendor?
- What is their level of cyber maturity?
- Are they subject to foreign ownership, control or influence?

The Cyber Centre also published 3 resources on supply chain risks for different audiences:

- [Cyber supply chain: An approach to assessing risk](#)<sup>30</sup> (overview for Canadians)
- [Protecting your organization from software supply chain threats](#)<sup>31</sup> (overview for managers)
- [The cyber threat from supply chains](#)<sup>32</sup> (threat bulletin for cyber security professionals)

### Protecting Canada's telecommunications infrastructure

Mobile networks form the backbone for how Canadians communicate, work and live online. CSE works closely with federal partners and Canadian telecommunications service providers (TSPs) to help keep those networks secure.

Evolving 5G technology will be able to support much faster connectivity and more powerful functions. However, there is also much greater scope for threat actors to exploit those networks.

In May 2022, the Government of Canada announced its intention to prohibit Huawei and ZTE products and services on Canadian 5G networks due to security concerns.

In June 2022, CSE outlined how we would evolve our [Security Review Program](#)<sup>33</sup> in light of this change. The program has worked with Canadian TSPs since 2013 to mitigate cyber security risks on their networks. This involved reviewing products and services from designated suppliers, including Huawei and ZTE. As a result, certain products were restricted from sensitive functions on Canadian networks.

Under the new Telecoms Cyber Resilience Program, CSE continues to work with Canadian TSPs to help them mitigate cyber security and supply chain risks. The program now considers **all** key suppliers and includes a new focus on network resilience.

### International standards

The Cyber Centre works closely with federal and international partners to develop and maintain international standards for IT products.

This year, we continued to certify commercial IT products under the:

- [Common Criteria](#)<sup>34</sup> program (cyber security standards)
- [Cryptographic Module Validation Program](#)<sup>35</sup> (cryptography standards)

We continued to work with international partners to develop standards for post-quantum cryptography (see [Cryptography](#) on page 22).

# Communications Security

Communications Security (COMSEC) is a big part of what CSE does. It's literally in our name. These efforts are ongoing, but never static. As technologies evolve, we update our methods and posture to ensure adversaries can't compromise the Government of Canada's sensitive communications.

## COMSEC

COMSEC refers to specific hardware, software, technologies, algorithms and procedures used to protect sensitive government communications. This year CSE continued to provide the Government of Canada with:

- secure phones, network encryptors and other COMSEC-enabled solutions for both national and international deployments
- cryptographic keys to protect sensitive communications and data
- advice and guidance to government and critical infrastructure regarding:
  - cryptography
  - EMSEC (Emissions Security)
  - OPSEC (Operational Security)
  - vulnerabilities
  - secure communications using commercial products

For example, we continued to support secure video-conferencing and mobile solutions for Cabinet and senior officials.

This year, the Cyber Centre saw an increase in secure communications requirements and the need for support in the critical infrastructure domain.

### COMSEC training

The Cyber Centre's Learning Hub runs mandatory training courses for users of Government of Canada COMSEC equipment. This year, the Learning Hub launched a new refresher course based on the most commonly-reported COMSEC incidents.

The Learning Hub continued to work with the Canadian Armed Forces and Department of National Defence to standardize COMSEC training across the Government of Canada.





## Cryptography

Cryptography is fundamental to COMSEC and cyber security. It ensures that data and communications can't be accessed without permission or altered by an adversary.

The threats to cryptography continue to evolve. Experts predict that as early as the 2030s, powerful computers using quantum physics may be able to crack the cryptography that we rely on today. If new cryptographic solutions that are resistant to these quantum computers are not developed and deployed worldwide, all digital information at rest or in transit may be at risk.

### New standards for post-quantum cryptography

The Cyber Centre is working with federal, commercial, academic and international partners to develop reliable post-quantum cryptography (PQC). PQC uses cryptographic techniques that are resistant to known attacks by quantum computers.

The international research effort on PQC took a big step forward in July 2022, when the US National Institute of Standards and Technology (NIST) [announced the first PQC candidates](#)<sup>36</sup> for standardization. The Cyber Centre has evaluated these candidates, ensuring that they provide sufficient security to protect information and systems of importance to Canada and Canadians.

NIST is expected to finalize the first PQC standards in 2024, after which the Cyber Centre will update our list of [approved cryptographic algorithms](#).<sup>37</sup> In the meantime, we have published new and updated guidance to help Canadian organizations prepare for the PQC transition:

- [Guidance on becoming cryptographically agile](#)<sup>38</sup>
- [Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information](#)<sup>39</sup> (updated with advice to phase out certain algorithms by 2023)

### Canada's National Quantum Strategy

In January 2023, Innovation, Science and Economic Development Canada (ISED) released [Canada's National Quantum Strategy](#).<sup>40</sup> It has 3 core aims:

- to make Canada a world-leader in quantum innovation
- to ensure the privacy and cyber security of Canadians in a quantum world
- to enable government and key industries to develop and quickly adopt quantum technologies

CSE contributed technical expertise to help form the strategy. Our experts will help to evaluate proposals under the strategy and to advise on their potential cyber security impact for the Government of Canada.



## Cyber security

CSE has a mandate to help protect Canada's federal institutions and critical infrastructure from cyber threats. The Cyber Centre is the government's operational lead for cyber security, working closely with Shared Services Canada and other federal partners. The Cyber Centre also draws on expertise from other parts of CSE including foreign signals intelligence.

### Budget 2022 investments

The cyber threat landscape is evolving rapidly. In response, [Budget 2022](#)<sup>41</sup> allocated new funds to enhance CSE's ability to:

- make critical government systems more resilient to cyber incidents
- prevent and respond to cyber attacks on critical infrastructure
- expand cyber security protection for small departments, agencies and Crown corporations
- prevent and defend against cyber attacks (see [Foreign cyber operations](#) on p.8)
- research emerging technologies (see [Research](#) on p.38)

These investments give CSE a strong foundation for growth. At the same time, we are working to expand our workforce to keep up with demand (see [Recruitment](#) on p.53).



### Protecting federal institutions

The Cyber Centre uses sensors, which are software tools installed in partner IT systems, to detect malicious cyber activity on government networks, systems and cloud infrastructure.

Our automated tools and expert analysts search the sensor data for unusual flows (patterns of network traffic) such as:

- attempts to deploy malware
- attempts to map systems and networks
- attempts to extract information

If we find malicious activity, we take action to thwart it. This includes directing our sensors to block it automatically.

This year, our automated defences protected the Government of Canada from 2.3 trillion malicious actions, an average of 6.3 billion a day.

Budget 2022 announced new funding for CSE to make critical government systems more resilient to cyber incidents. On a cash basis, this funding amounts to:

- \$312.9 million over 5 years, starting in 2022 to 2023, and \$61.7 million ongoing<sup>42</sup>

### Sensor deployments as of March 2023:

- Host-based sensors (HBS)
  - 85 federal institutions (up from 79 in 2022)
  - 860,000 devices (up from 730,000)
- Cloud-based sensors (CBS)
  - 72 federal institutions (up from 70)
- Network-based sensor (NBS)
  - 84 federal institutions benefit from our sensor deployed at the network perimeter
- Virtual network-based sensors (see [Protecting the cloud](#) on p.24)
  - 5 federal institutions

## Protecting the cloud

MapleTap is a cloud network-based sensor that can be deployed directly in partner infrastructure. Like our other sensors, the technology was designed by the Cyber Centre to detect and defend against suspicious cyber activity. It first rolled out in January 2022 and, as of March 2023, has 10 unique deployments across 5 federal institutions.

The MapleTap tool is available on the public cloud marketplace. Cyber defenders can use the tool and build on it to strengthen their cyber defence capabilities. The Cyber Centre also works closely with cloud vendors. As an example, in October 2022, one of the main cloud vendors recognized the MapleTap team for having uncovered and disclosed a networking vulnerability to them. This is one of many examples where the Cyber Centre helps strengthen cloud services for millions of users worldwide.

## Crown corporations and smaller departments and agencies

A [2022 report by the National Security and Intelligence Committee of Parliamentarians](#)<sup>43</sup> highlighted the vulnerability of Crown corporations and smaller departments and agencies (SDAs) whose IT infrastructure is outside the government's network defences. It recommended maximizing the number of federal institutions using CSE's sensors to detect cyber threats on their networks.

The Cyber Centre has conducted extensive outreach to this sector over the last 3 years. Since March 2020, the number of Crown corporations and SDAs signed up for our sensors has grown from 12 to 37 (out of 86).

The Cyber Centre continues to view this sector as a high priority and is working to onboard more federal institutions to our services.

The running total of Crown corporations and smaller departments and agencies signed up for CSE's sensor program as of March 31 each year was as follows:

- March 2023:
  - Crown corporations: 11
  - SDAs: 26
- March 2022:
  - Crown corporations: 10
  - SDAs: 22
- March 2021:
  - Crown corporations: 5
  - SDAs: 19
- March 2020:
  - Crown corporations: 1
  - SDAs: 11

Budget 2022 proposed new funding to expand cyber security protection for small departments, agencies and Crown corporations. On a cash basis, this funding amounts to:

- \$57.5 million over 5 years, starting in 2022 to 2023 and \$12.8 million ongoing<sup>44</sup>

## Non-federal deployment of host-based sensors

This year, the Cyber Centre also deployed over 5100 host-based sensors to protect a non-federal institution that was experiencing a serious cyber incident. This emergency rollout was authorized by the Minister of National Defence. The *CSE Act* allows the Minister to designate non-federal systems as being of importance to the Government of Canada. This authorizes CSE to take action to defend them under our cyber security mandate.

## Security posture dashboard

ObservationDeck is an interactive web application that helps Government of Canada departments to better understand their cyber security posture.

Each partner can see curated daily cyber threats that apply to the assets on their network. In the event of a cyber incident, ObservationDeck also lets Cyber Centre analysts get a quick view of assets that may have been compromised.

Historically, ObservationDeck included sensor data from:

- host-based sensors (HBS)
- network-based sensors (NBS)
- select threat data feeds

This year ObservationDeck was expanded to include data from our cloud-based sensors (CBS).

The running total of Government of Canada departments with ObservationDeck as of March 31 each year was as follows:

- March 2023:
  - Departments: 57
    - with CBS: 53
- March 2022:
  - Departments: 50
    - with CBS: 0

## Working with critical infrastructure

We know that Canada's critical infrastructure is a target for cyber threat activity.

Cyber incidents in these key sectors can cause major disruption and put health and safety at risk.

In the spring of 2023, the Cyber Centre put out a cyber flash to partners. It concerned a confirmed report that a cyber threat actor had the potential to cause physical damage to Canadian critical infrastructures. There was no physical damage, but the threat is real and ongoing.

Budget 2022 announced new funding to enhance CSE's abilities to prevent and respond to cyber attacks on critical infrastructure. On a cash basis, these funds amount to:

- \$185.5 million over 5 years, starting in 2022 to 2023, and \$40.6 million ongoing<sup>45</sup>

**Critical infrastructure is still a prime target for both cybercriminals and state-sponsored actors alike.**

[National Cyber Threat Assessment 2023-2024<sup>45</sup>](#)

## Cyber security

### Sectors

This year, the Cyber Centre's partnerships team engaged with almost 1400 critical infrastructure organizations (up from around 1000 the year before). These partners belong to the following sectors:

- Academia
- Crown corporations
- Democratic institutions
- Energy
- Finance
- Food / water / manufacturing
- Health
- Information and communications technology
- Provinces / territories / municipalities
- Small and medium organizations
- Transport

The team dedicated to food, water and manufacturing is new this year.

### Energy infrastructure

The Cyber Centre continues to work with partners in the energy sector to share cyber threat information and strengthen cyber security.

Ongoing collaborations include:

- the [Blue Flame Program](#)<sup>47</sup> (with the Canadian Gas Association)
- the [Lighthouse](#)<sup>48</sup> initiative (with Ontario's Independent Electricity System Operator)

Participating organizations share network data with the Cyber Centre and receive customized threat reports in return.

More energy sector partners joined these initiatives this year. The Cyber Centre is working to upgrade and evolve these programs in the coming fiscal year.

### Assessing needs

In October 2022, Public Safety Canada released an updated version of the [Canadian Cyber Security Tool](#).<sup>48</sup> CCST 2.0 was developed in collaboration with the Cyber Centre and is aimed at critical infrastructure providers. The virtual tool helps organizations assess their technical resilience compared to current best practice. The data, gathered by Public Safety Canada, also helps to identify where the most common resilience gaps are. This will help the Cyber Centre plan our resources to close those gaps.



### Pilot program for municipalities

Municipalities are a popular target for ransomware attacks. They have large threat surfaces (many devices, users and data) but often their cyber security budgets are relatively small.

This fiscal year, Public Safety Canada and the Cyber Centre ran a pilot program to help Canadian municipalities identify gaps in their cyber security.

18 municipalities performed a virtual self-assessment of their cyber security using the CCST 2.0. Cyber Centre advisors then walked them through the results, helping them to identify priorities and draw up action plans. One of the municipalities developed an in-depth action plan which it has offered to share with other municipalities across Canada.

## Incident management

**Cyber Incident: Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.**

Canadian Centre for Cyber Security,  
[Glossary](#)<sup>50</sup>

When cyber incidents occur on federal networks or Canadian critical infrastructure, the Cyber Centre is there to help.

Cyber incidents can range from basic phishing attempts to sophisticated activity by advanced persistent threat actors. They may or may not result in compromises.

Our incident management team offers expert advice and guidance to help the victim's IT team mitigate any damage and get systems back online. Once the incident has been resolved, the Cyber Centre follows up to help the victim identify and address vulnerabilities in their IT setup.

This year, the Cyber Centre opened 2089 cyber security incident cases. Of those victims, 957 were federal institutions and 1132 were critical infrastructure organizations.

In some cases, the cyber incident response team deployed to assist other government organizations in Canada as well as systems of importance to the Government of Canada.

The number of cyber incident cases opened by the Cyber Centre for the last 3 fiscal years were as follows:

- 2022 to 2023:
  - total cases: 2089
    - federal institutions: 957
    - critical infrastructure: 1132
- 2021 to 2022:
  - total cases: 2195
    - federal institutions: 1152
    - critical infrastructure: 1043
- 2020 to 2021:
  - total cases: 2047
    - federal institutions: 881
    - critical infrastructure: 1166

(Statistics for previous years have been updated to ensure consistent methodology with this year's numbers.)

These statistics are only a fraction of the whole. The vast majority of cyber incidents go unreported. Yet cyber threat actors never stop at just one victim. CSE urges Canadian organizations to [report cyber incidents](#)<sup>51</sup> to law enforcement and to the Cyber Centre so that we can:

- offer advice and guidance
- warn other organizations

### International networks

The Cyber Centre is Canada's national Computer Security Incident Response Team (CSIRT). We work with other national CSIRTs around the world to exchange information, helping each country to prepare and respond more effectively to cyber threats.

This year, the Cyber Centre joined the CSIRTAmericas Network, a community of 36 CSIRTs from 21 countries across the Americas.

Networks like CSIRTAmericas act as important sharing hubs to improve our collective cyber security.

## Cyber security

### Cyber threat intelligence

CSE's cyber threat intelligence program is focused on delivering foreign intelligence on cyber threats to Canada and its interests.

This year, the program continued to uncover, investigate, and monitor the tactics, techniques and procedures employed by sophisticated state-sponsored actors, non-state actors, and cybercriminals.

The program helps to counter these activities by providing timely and actionable intelligence on how these malicious actors operate.

This helps to protect federal systems, Canadian critical infrastructure, our allies and other systems of importance to the Government of Canada.

### Sharing cyber threat information with partners

The Cyber Centre shares cyber threat information with government and critical infrastructure partners in various ways.

#### Automated threat intelligence feed

Aventail is the Cyber Centre's automated threat intelligence sharing service. It shares technical details about cyber threat activity known as indicators of compromise (IOCs). These can include malicious:

- web domains
- web URLs
- IP addresses
- file hashes

We vet these IOCs and share them with partners in government and critical infrastructure so they can defend against these known threats on their networks. (CSE takes care to ensure that partners meet our legal and policy requirements before they are onboarded to Aventail.)

In addition, the Cyber Centre provides Aventail to several partner organizations via re-sharing agreements. This allows those organizations to leverage Aventail to help protect all Canadians (see [Helping Canadians to protect their devices](#) on p.36).

Until this year, only partners with a dedicated server could ingest Aventail. In December 2022 the Cyber Centre launched a web application so that smaller critical infrastructure organizations can also access our threat feed. New partners can sign up for the machine-to-machine feed, the web application, or both.

This fiscal year, Aventail shared over 37,000 unique IOCs. That's an average of just over 100 a day.

The running total of organizations subscribed to Aventail as of March 31 each year was as follows:

- March 2023:
  - total partners: 152
    - federal institutions: 20
    - critical infrastructure: 132
- March 2022:
  - total partners: 120
    - federal institutions: 13
    - critical infrastructure: 107



## Notifications

The Cyber Centre sends out different types of notifications to the cyber security community.

On our website and social media we publish:

- advisories: on routine cyber security issues
- alerts: on critical vulnerabilities

Cyber Centre partners can also sign up to receive:

- cyber flashes: urgent notifications delivered via email containing sensitive information that cannot be shared publicly
- National Cyber Threat Notification Service (NCTNS): daily updates about malware and vulnerabilities on a partner's IP space
- scorecards: a monthly summary of NCTNS data showing how a subscriber's cyber hygiene ranks against anonymized peers in their sector

This year the Cyber Centre issued:

- 737 advisories
- 21 alerts
- 14 cyber flashes

The number of organizations signed up for notification services as of March 31, 2023, was as follows:

- cyber flashes: 960 organizations (up from around 790 the previous year)
- NCTNS: over 1000 (up from around 750)
- scorecards: 214 (up from 179)

## Community engagement

This year, the Cyber Centre continued to engage critical infrastructure partners through:

- cyber threat briefings:
  - bi-weekly video calls hosted by the Cyber Centre, regularly attended by over 600 partners
  - sector-specific community calls: hosted by industry partners, attended by Cyber Centre experts
- 10 Walk-the-Talk briefings: 30-minute technical deep-dives on a single topic
- 161 public speaking engagements

## Malware analysis

[Assemblyline](#)<sup>52</sup> is the Cyber Centre's malware detection and analysis platform.

Partners and defence sensors submit suspicious files for analysis. Assemblyline analyzes them using advanced malware detection technologies and provides a result within minutes, along with details to help inform the response.

This year Assemblyline scanned over 1 billion suspicious files.

The running total of organizations subscribed to Assemblyline as of March 31 was as follows:

- March 2023:
  - total partners: 228
    - Government of Canada: 45
    - critical infrastructure: 183
- March 2022:
  - total partners: 165
    - Government of Canada: 32
    - critical infrastructure: 133

Malware is constantly evolving, and threat actors are always devising new methods to deliver it. Therefore, our analysts work year-round to add new detection capabilities to Assemblyline based on the latest malware types and methods.

## Advice to government and critical infrastructure

The Cyber Centre is Canada's technical authority for cyber security.

We provide advice to Government of Canada departments on how to protect their IT assets, the information they hold, and the services they provide to Canadians.

For example, we are advising Employment and Social Development Canada (ESDC) on a multi-year project to transform the way benefits are delivered. The goal is to build a user-friendly digital platform that will simplify and speed up the way Canadians apply for and receive benefits like EI and Old Age Security. Ensuring stringent cyber security standards from the start will help ensure the new platform:

- is resilient to ransomware and other cyber attacks
- keeps Canadians' personal information secure

## Cyber security

The Cyber Centre also advises Canadian critical infrastructure (CI) providers on cyber security issues that affect them.

For example, this year we began building a community of interest around cyber security for industrial control systems (ICS). These are electronic systems used to control machinery or industrial processes. When connected to the Internet, they represent a high-value target for cyber threat actors. As of March 2023, around 40 government and industry partners had joined the community of interest. This helps us to better understand their needs and offer in-depth cyber security advice.

**ICS is a high-value target for threat actors because they can cause real world effects, ranging from annoyances (e.g. turning on and off lights) to life threatening and costly events (e.g. equipment malfunctions and permanent damage).**

The Cyber Centre, [Security Considerations for Industrial Control Systems](#)<sup>53</sup>

## Cyber security training

The Learning Hub offers training for government and critical infrastructure employees in cyber security and Communications Security (see [COMSEC](#) on p.21).

Before the pandemic, the Learning Hub offered only in-person training. Over the last 3 years it has also developed a catalogue of self-paced eLearning courses and virtual versions of instructor-led courses. This has allowed the Learning Hub to reach more learners across Canada.

Attendance at eLearning courses this fiscal year was almost 4 times higher than the previous year. Overall Learning Hub attendance more than doubled. The Learning Hub created a new team to work on improving the online learning experience for our users.

### The Learning Hub in 2022 to 2023:

- 8422 participants (up 123%)
- Format:
  - 70% eLearning
  - 30% instructor-led (virtual and in-person)
- Audience:
  - 98% Government of Canada
  - 2% critical infrastructure

### Training for public servants

To help keep government systems secure, it's important for all public servants to practice good cyber hygiene. This year the Cyber Centre worked with the Canada School of Public Service to co-develop the [Discover Cyber Security learning path](#).<sup>54</sup> It includes:

- a new online course: Discovering Cyber Security
- 3 existing instructor-led courses
- Get Cyber Safe videos and resources
- Cyber Centre guidance publications

The Learning Hub also launched a one-day instructor-led course on Cyber Security Best Practices for both public servants and critical infrastructure employees.



## Promoting digital resilience for Canadians

The Cyber Centre helps to protect Canadians from cyber threats by raising awareness, working with partners to identify and remove threats, and promoting cyber skills.

### Get Cyber Safe

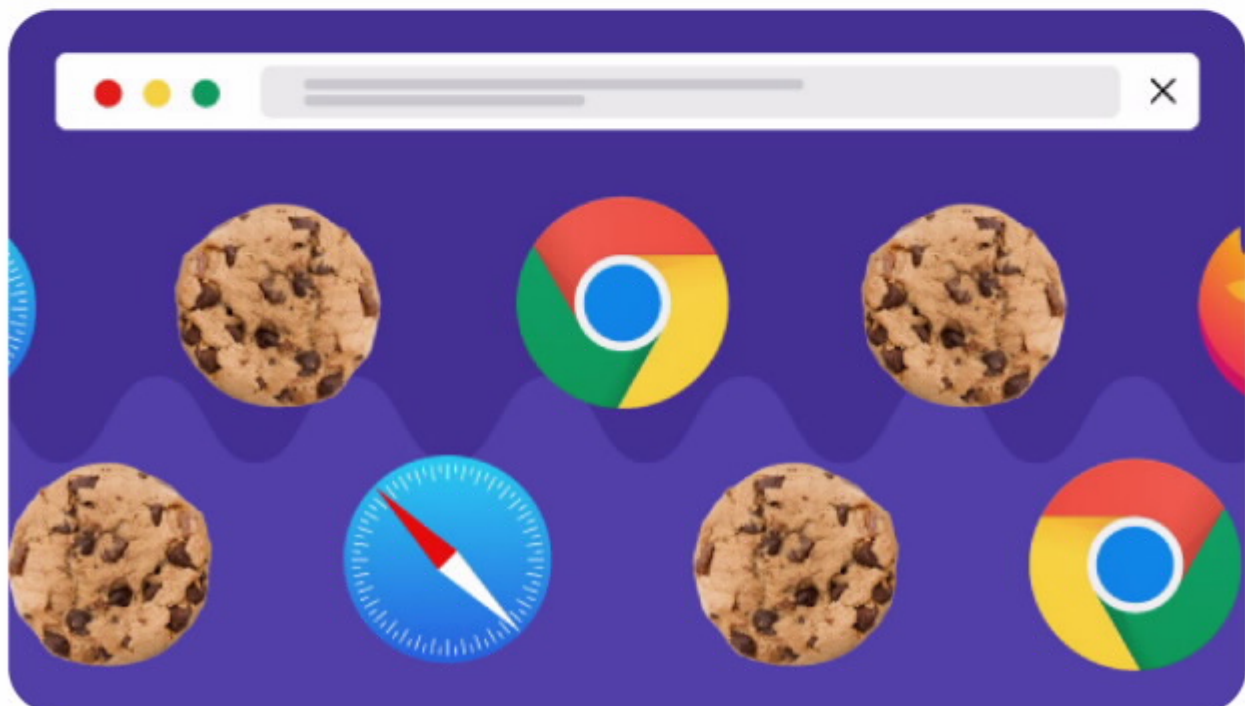
[Get Cyber Safe](#)<sup>55</sup> is a national public awareness campaign to inform Canadians about the simple steps they can take to help protect themselves online.

This year Get Cyber Safe continued to promote its most popular resources to help Canadians with cyber security in their daily lives. We also produced approximately 50 new pieces of content, such as:

- [How to secure your online financial transactions](#)<sup>56</sup>
- [What to know about Internet cookies](#)<sup>57</sup>
- [Spot the signs of a catfish on dating platforms](#)<sup>58</sup>
- [What to do if you are a victim of a phishing scam](#)<sup>59</sup>

Get Cyber Safe worked on 6 major campaigns throughout the year:

- Cyber security awareness for older adults (June)
- Back-to-school campaign for post-secondary students (September)
- Cyber Security Awareness Month (October)
- “Don’t get reeled in” advertising campaign (October)
- Get Cyber Safe holiday campaign (November - January)
- Fraud Prevention Month (March)



## Promoting digital resilience for Canadians

### Cyber Security Awareness Month

Cyber Security Awareness Month (Cyber Month) is held each year in October. The theme for 2022 was “Fight phishing: Ruin a cyber criminal’s day”.

Get Cyber Safe produced multiple [Cyber Security Awareness Month resources](#),<sup>60</sup> including a toolkit for champions, blogs, infographics, videos, an interactive phishing quiz and a catchy [phishing shanty jingle](#).<sup>61</sup>

7 partners worked with Get Cyber Safe to co-create content:

- Canada Revenue Agency
- Innovation Science and Economic Development Canada
- Cadets Canada
- Canadian Bankers Association
- Insurance Bureau of Canada
- Microsoft Canada
- National Cybersecurity Alliance and CybSafe

350 champions shared Cyber Month content with their audiences (up from 247 in 2021).

In total, our campaign content was seen over 350,000 times, down slightly from 390,000 impressions in 2021.

### “Don’t get reeled in” advertising campaign

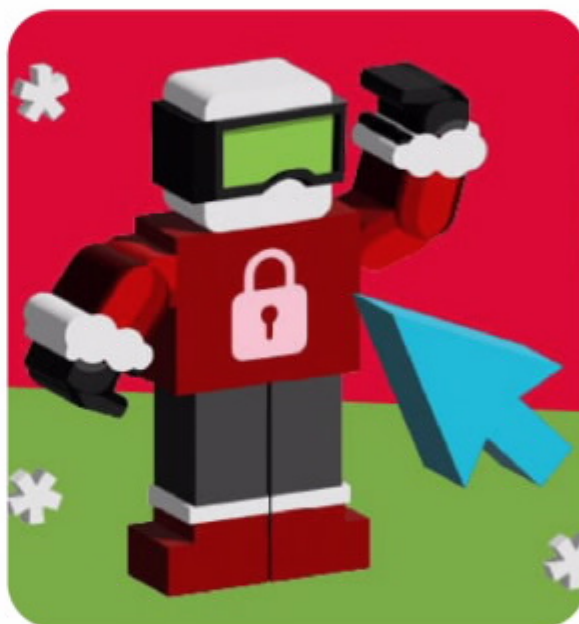
To coincide with Cyber Month, Get Cyber Safe ran an advertising campaign about phishing under the tag line “[Don’t get reeled in](#)”.<sup>62</sup> The campaign ads were seen over 47 million times, including 6.1 million video views. The campaign drove a three-fold increase in visits to the Get Cyber Safe website during the month of October 2022 (124,000 total visitors; compared to 39,000 in October 2021).

### Get Cyber Safe holiday campaign

During the holiday season, Get Cyber Safe worked with strategic partners including the Canadian Anti-Fraud Centre (CAFC) and the RCMP to create content such as:

- [Federal partners remind Canadian consumers to be vigilant for cyber threats this Black Friday and Cyber Monday](#)<sup>63</sup> (with CAFC and the RCMP)
- [Top 12 scams of the holiday season](#)<sup>64</sup> (with CAFC)
- [Adopt meaningful gaming habits this holiday season](#)<sup>65</sup> (with the gaming platform, Roblox)

Get Cyber Safe also launched the first [Unboxing Day](#)<sup>66</sup> devoted to securing new devices.



### Fraud Prevention Month

For Fraud Prevention Month, in March 2023, Get Cyber Safe worked with the RCMP and the CAFC to produce resources about the most common online fraud techniques, including:

- [investment scams](#)<sup>67</sup>
- [spear phishing](#)<sup>68</sup>
- [service scams](#)<sup>69</sup>
- [phishing](#)<sup>70</sup>
- [what's in a fraudster's toolbox](#)<sup>71</sup>

Building meaningful relationships continues to be a priority for Get Cyber Safe to increase its reach to Canadians across the country.

## Promoting digital resilience for Canadians

### Reports and guidance

The Cyber Centre publishes threat reports and guidance resources online so that all Canadians and Canadian organizations can access high-quality cyber security information.

In October 2022, the Cyber Centre published the [National Cyber Threat Assessment 2023-2024](#)<sup>72</sup> (NCTA).

This flagship report is published every 2 years. It draws on classified and unclassified sources to identify key trends in the cyber threat landscape. This edition of the report focused on 5 trends:

- Ransomware
- Threats to critical infrastructure
- State-sponsored cyber activity
- Online disinformation
- Disruptive technologies

To accompany the NCTA, we published [guidance](#)<sup>73</sup> to address those 5 trends and updated our [Introduction to the Cyber Threat Environment](#).<sup>74</sup>

In total this year, the Cyber Centre issued:

- 4 reports and assessments
- 51 advice and guidance publications
  - 40 new
  - 11 updated

### Website renovation

In May 2022, we overhauled the [Cyber Centre website](#)<sup>75</sup> to make it more accessible for users with disabilities, and to make it easier for users to find the content relevant to them. The home page now allows users to select information for:

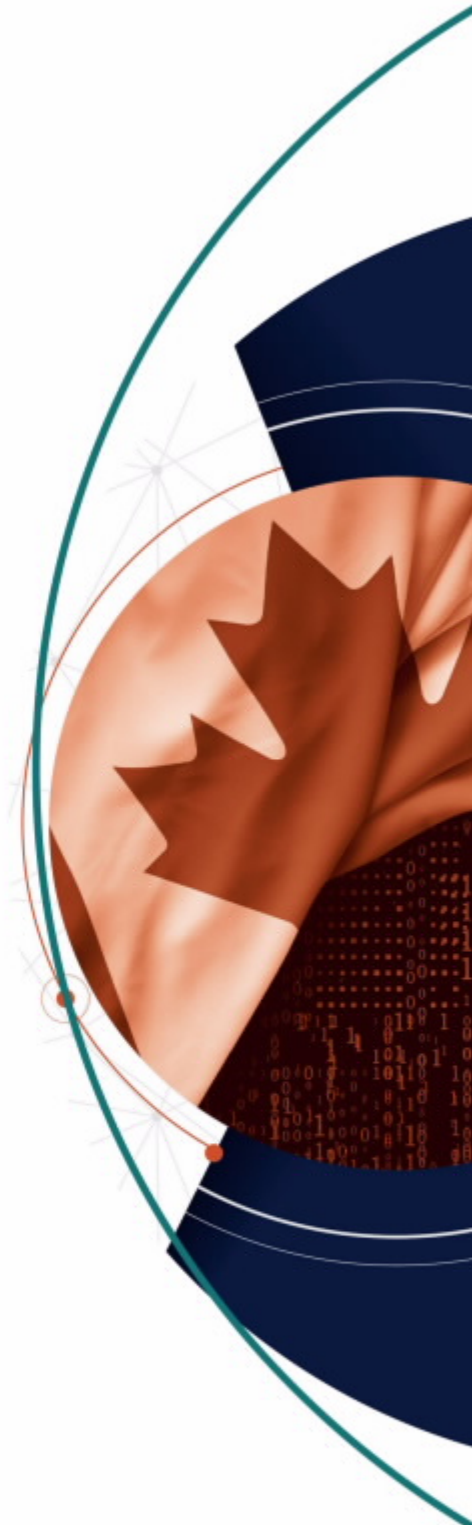
- individuals
- small and medium businesses
- large organizations and infrastructure
- government institutions
- academia

The “Report a cyber incident” button is easier to find at the top of the home page. It now directs individual Canadians more clearly to the right agency for their situation.

### Social media

Social media is one of the most important ways CSE shares information with Canadians, including many of the highlights mentioned in this report such as:

- exposing Russian disinformation campaigns
- Cyber Security Awareness Month
- the National Cyber Threat Assessment



## Promoting digital resilience for Canadians








### Social media by the numbers

CSE, the Cyber Centre and Get Cyber Safe each have their own social media presence. They have a combined total of 17 accounts across 5 social media platforms.

This fiscal year, content from these accounts was seen more than 5.2 million times (down from 6.6 million the previous year).

Our overall number of followers increased from 172,500 to 184,000.

As of March 31, 2023, the combined number of English and French followers for each account (rounded to the nearest thousand) were as follows:

Platform	Account	Followers	Change
	CSE	22,000	Up 5%
	Cyber Centre	32,000	Up 18%
	Get Cyber Safe	54,000	Down 1.8%
	Get Cyber Safe	52,000	No change
	CSE	15,000	Up 50%
	Get Cyber Safe	2,000	No change
	CSE	3,000	Up 50%
	Get Cyber Safe	3,000	No change
	CSE	1,000	Up 100%

## Finding malicious domains

Domains are like neighbourhoods on the Internet. Canada.ca is a domain. Threat actors use malicious domains to conduct activities like:

- hosting spoof websites
- sending phishing emails
- spreading malware

The Cyber Centre finds these malicious domains in various ways, including:

- open-source and commercial threat feeds
- sensor data from government networks
- cyber incidents reported to the Cyber Centre
- proactive cyber threat hunting
- submissions from industry partners (see [Protecting Canadians from phishing and smishing](#) on p.35)

After vetting the information and removing duplicates, the Cyber Centre takes steps to mitigate the threat of malicious domains, including:

- blocking them on Government of Canada networks
- sharing the details in our threat feeds
- directing trusted partners to block or remove them from the Internet (see [Mitigations](#) on p.36)

## Protecting Canadians from phishing and smishing

One of the most common ways threat actors try to get Canadians to visit malicious domains is through phishing (emails) and smishing (texts). These messages often contain links to malicious domains to trick you into sharing passwords or credit card details. They may also install malware onto your device.

Critical infrastructure providers play an essential role in protecting Canadians against phishing and smishing, particularly in the finance, IT and telecommunications sectors.

The Cyber Centre has worked with key partners in this sector since 2019 to gather malicious content for analysis. No user information is shared with the Cyber Centre under this initiative, only the content of the message itself.

In 2021, the Cyber Centre launched Fox, a platform to ingest data from partners more easily. This year partners used Fox to submit approximately:

- 850,000 URLs (web links):
- 274,000 of which were malicious
  - 12,700 of which were new discoveries

The Cyber Centre shares these URLs with participating partners so they can also use them to help protect their customers.

## The most common scam types submitted by partners this year



## Promoting digital resilience for Canadians

### Mitigations

During the pandemic, the Cyber Centre began working with trusted commercial partners to remove websites and email domains imitating federal entities.

In July 2021, we expanded our mitigation requests to include other sources of malicious content. This includes those shared with us by critical infrastructure partners (see [Protecting Canadians from phishing and smishing](#) on p.35).

The number of malicious domains blocked or removed by our partners in each of the last 3 fiscal years was as follows:

- 2022 to 2023:
  - Government of Canada spoofs: 3167
  - other malicious domains: 306,000
- 2021 to 2022:
  - Government of Canada spoofs: 2943
  - other malicious domains: 312,000
- 2020 to 2021:
  - Government of Canada spoofs: 7348
  - Other malicious domains: 0

### Helping Canadians to protect their devices

The Cyber Centre has an ongoing partnership with the non-profit agency CIRA to help Canadians protect their personal devices from malware and phishing.

CIRA Canadian Shield is a free service that protects Canadians' privacy while browsing. It has a threat-blocking option that prevents users from connecting to malicious websites. It can be downloaded as a mobile app or used to configure personal devices including home routers. The block list for Canadian Shield uses Cyber Centre threat intelligence combined with data from other CIRA partners.

This fiscal year, the number of users signed up for Canadian Shield's threat-blocking services grew from 177,000 to over 279,000. The service recorded more than 215 million blocks from March 2022 to March 2023.



## Community outreach

CSE's community outreach program is about inspiring young Canadians to get passionate about technology and coding. We want to help build a strong cyber workforce across Canada.

We are particularly interested in reaching young people who are under-represented in tech, including girls, non-binary students and Black and Indigenous youth.

This year, CSE volunteers were able to resume in-person outreach events including:

- 7 Raspberry Pi workshops in 3 Ottawa schools
- Cyber Days activities for 2 gifted classes in Ottawa (with the Information and Communications Technology Council)

We participated in hack-a-thons and other virtual events with our partners:

- Hackergal
- CyberTitan

We initiated 3 new partnerships with:

- Actua
- Black Boys Code
- University of Ottawa Department of Mathematics and Statistics

**Thank you very much for your dedication to launching this cyber security opportunity for our students! There wasn't a single child who didn't learn something new - lots new in fact. Every student was engaged in the challenging activities and many are thinking about a future in IT. What a win!**

Program for Gifted Learners  
teacher, Ottawa Catholic  
School Board

## Working with Indigenous partners

The Cyber Centre is working with Indigenous partners to help strengthen cyber security in their communities.

Throughout the year, the Cyber Centre gave cyber security briefings to many organizations across Canada, including territorial governments and Indigenous organizations.

CSE shared cyber security resources and built connections with Indigenous organizations at:

- the Indigenous Technology Summit (Halifax, September 2022)
- the Assembly of First Nations Special Chiefs Assembly (Ottawa, December 2022)
- the Inuit Technology Forum (Iqaluit, March 2023)

In June 2022, the Cyber Centre hosted the [Cyber\\*Sci Canadian finals](#).<sup>76</sup> Cyber\*Sci is a non-profit that works with young cyber talent across Canada. At CSE's request, this year's competition featured its first all-Indigenous team. The event helped to showcase participants' skills and build their professional networks.

## Promoting cyber talent

Canada needs more cyber security professionals.

The Cyber Centre supported the development of cyber skills in Canada this year by:

- advising academic institutions on curriculum content
- producing cyber security resources for students and teachers
- working with partners in industry and academia to identify skills gaps
- updating resources including:
  - the [Cyber Security Career Guide](#)<sup>77</sup>
  - [Certifications in the field of cyber security](#)<sup>78</sup>



**The number of jobs for cyber security professionals in Canada continues to grow year after year. This trend is not unique to Canada, there are millions of vacant cyber security positions available around the world.**

[Cyber Security Career Guide](#)<sup>78</sup>



## Innovation

Technology evolves quickly. To keep up, CSE promotes a culture of constant innovation, including research and collaborative events.

## Research

CSE conducts research as part of our mission to help protect Canada and contribute to the overall cyber security community.

Budget 2022 proposed new funding to enhance Canada's cyber security capabilities through research investment. CSE has since been approved for \$44.5 million over 9 years to fund academic research on cutting-edge technologies relevant to CSE's activities.

This significant investment will allow us to expand our research activities and strengthen our capabilities.



## Tutte Institute for Mathematics and Computing

Researchers at CSE's [Tutte Institute for Mathematics and Computing \(TIMC\)](#)<sup>80</sup> work with CSE colleagues, Five Eyes partners, academia and industry to tackle the hardest scientific challenges related to our mission.

A particular focus this year was the topic of foreign influence campaigns on social media. CSE researchers produced a comprehensive "problem book" outlining challenges in detecting malicious foreign influence campaigns and delivered tools to detect coordinated activity.

Other research activities included:

- developing data maps and conducting exploratory data analysis
- engaging industry partners to develop and pilot methods for secure computation in insecure environments
- improving tools and workflows to enable ethical and robust data science that can easily be reproduced and interpreted
- conducting research to support the post-quantum cryptography standardization processes

TIMC contributed back to the external academic community by:

- organizing 2 conferences
- giving 6 research presentations
- participating in 7 special workshops and conference panels
- publishing in more than 10 journal articles, conference proceedings and textbooks
- leading panels on equity, diversity and inclusion in STEM
- speaking at local universities
- sitting on the board of the Canadian Mathematical Society

Software libraries from TIMC averaged over 2.5 million downloads per month over the course of the year.

In November 2022, the Museum of Modern Art displayed art that was generated using the [UMAP algorithm](#),<sup>81</sup> a technique developed by one of our researchers.

“It's stunning to see my work used at MoMA. There are deep connections between abstract mathematics and art, and Refik Anadol's work concretely realizes this interplay.”

Leland McInnes, CSE researcher, via [Artnet News](#)<sup>82</sup>

## Applied research

Our researchers working in [applied research](#)<sup>83</sup> explore the current and incoming challenges we face in carrying out CSE's mission. We build solutions to enhance our capabilities.

This year, we developed the following products using data science to support the work of CSE analysts:

- An **automated translation software for mission-critical languages** that's faster and more accurate than previously available methods. It uses machine learning and was created in collaboration with partners in SIGINT.
- A **suite of image analysis services** to process, enrich and search our data collection.
- **Tools to triage mission data** using data science tools to analyze text and identify topics.
- **Tools that allow for foreign intelligence/SIGINT analysts** to better understand and detect influence and effects.

We also created a new malware detection module for files that are used to perform various functions or operations on a computer. The module has been added to CSE's externally available [AssemblyLine](#)<sup>84</sup> tool for file triage and malware analysis.

## Innovation

---

### Vulnerability research

As part of our mandate, CSE conducts [vulnerability research](#)<sup>85</sup> to find cyber security weaknesses that could be exploited by threat actors. We use the [CSE Equities Management Framework](#)<sup>86</sup> to determine whether disclosing a vulnerability is in the best security interests of Canada and Canadians.

This year, our researchers:

- discovered several high-impact vulnerabilities and disclosed them to the affected vendors
- launched a new initiative to explore cyber security concerns associated with a broader range of Internet of Things software and hardware

We increased our academic engagement and outreach activities in the vulnerability research space to reach emerging technical talent across Canada.

As in previous years, many CSE researchers made contributions to CSE collaborative events, such as Big Dig and GeekWeek.

### Collaborative events

---

CSE promotes innovation through cyber security workshops and other collaborative events. Partners from government, industry, academia and international allies work together on current and future problems related to CSE's mission.

#### GeekWeek

GeekWeek is the Cyber Centre's unclassified cyber security workshop.

Held from April to May 2022, GeekWeek 7.5 was fully virtual due to pandemic restrictions.

Teams explored many topics, including:

- enhancing our malware analysis capabilities
- reducing the number of false positives in cyber threat detection
- improving the cyber security of:
  - cloud infrastructure
  - Internet of Things (IoT) devices
- exploring ways malicious actors could exploit:
  - 5G telecommunications infrastructure
  - connected vehicles
- researching cryptocurrencies in relation to malicious activity and money laundering
- using machine learning to identify phishing emails

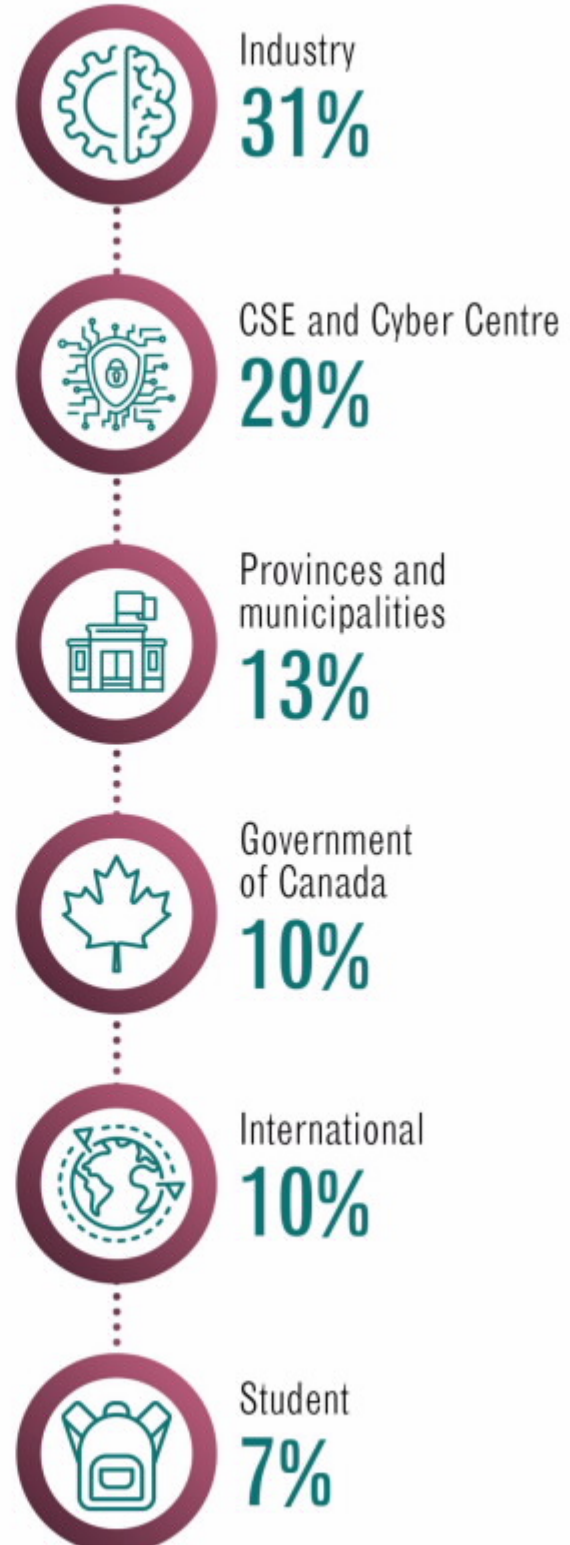
The Cyber Centre works year-round to innovate and develop new systems and techniques to improve Canada's cyber resilience.



### GeekWeek 7.5 by the numbers



### GeekWeek 7.5 by sector



## Innovation

### Big Dig

Big Dig is CSE's annual classified cyber security workshop.

For 2 weeks, teams collaborate to find new solutions to real-world problems.

Participants come from CSE, private industry, other Government of Canada departments and Five Eyes partner agencies.

This year, a record number of industry and Five Eyes partners took part.

Because teams use CSE's classified systems and tools, all participants must hold a valid security clearance.

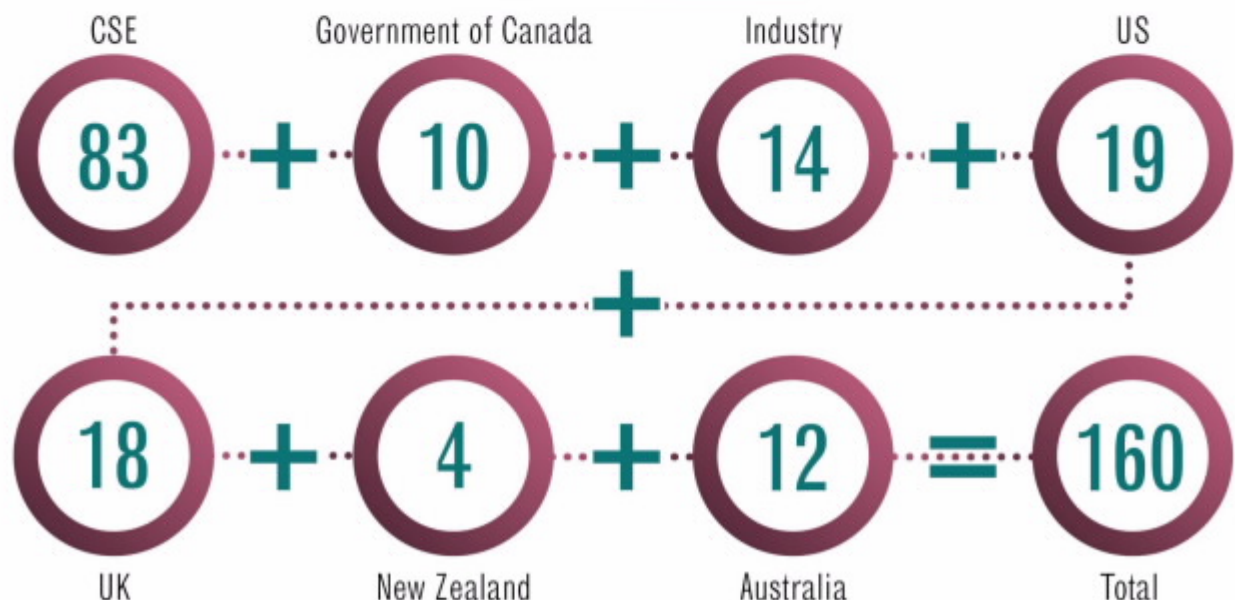
Teams worked on proof-of-concept solutions to various problems, including how to:

- speed up detection and mitigation of malware on Government of Canada networks
- ensure those networks stay protected:
  - in the cloud
  - in a hybrid work environment
- build an analysis platform "in a box" to deploy to non-government victims of cyber attacks
- better protect Internet-connected devices such as:
  - Industrial Control Systems
  - Smart devices

**I am so pleased to see so many of the brightest minds in this field gathered in one place. To collaborate and challenge yourselves to solve complex problems, and help improve our collective cyber resilience.**

Anita Anand, Minister of National Defence,  
Big Dig keynote speech,  
November 2022

### Big Dig participants 2022



## Accountability

Strict internal and external mechanisms exist to ensure CSE's activities comply with the law and respect the privacy of Canadians.

Note that in this chapter, some statistics are given by calendar year to match with our oversight and review bodies.

### Ministerial Authorizations

Ministerial Authorizations (MAs) are legal instruments that allow CSE to carry out certain activities under our mandate. There are 4 types of authorization:

- Foreign Intelligence
- Cybersecurity
- Active Cyber Operations
- Defensive Cyber Operations

#### Foreign Intelligence and Cybersecurity Authorizations

The Minister of National Defence must authorize any foreign intelligence or cyber security activities that could:

- contravene an act of Parliament, or
- interfere with a reasonable expectation of privacy of a Canadian or person in Canada

For example, any activities that risk incidentally intercepting the private communication of a Canadian or anybody in Canada must first be authorized by the Minister.

The Intelligence Commissioner must also approve Foreign Intelligence Authorizations and Cybersecurity Authorizations before the activities can begin. Each authorization is valid for up to a year.

In 2022, CSE submitted a total of 6 MAs to the Intelligence Commissioner:

- 3 Foreign Intelligence Authorizations
- 1 Cybersecurity Authorization (to help protect federal institutions)
- 2 Cybersecurity Authorizations (to help protect non-federal institutions)

The Intelligence Commissioner fully approved 5 authorizations and partially approved 1 authorization related to cyber security for a federal infrastructure. In this case, the Intelligence Commissioner approved the authorization with the exception of one activity, concluding that there was not enough information to establish whether the activity was covered by the *CSE Act*.

A summary of these conclusions can be found in the Intelligence Commissioner's [2022 Annual Report](#).<sup>87</sup>

When an authorization is partially approved, CSE only carries out the approved activities.

CSE welcomes the Intelligence Commissioner's perspective on how to improve the Ministerial Authorization process. We continue to use the comments in his decision letters to inform the next annual cycle of Ministerial Authorizations.



## Accountability



### Foreign cyber operations authorizations

Foreign cyber operations (FCO) is an umbrella term for activities conducted under the active cyber operations (ACO) and defensive cyber operations (DCO) aspects of [CSE's mandate](#).<sup>88</sup> FCO authorizations permit CSE to conduct a variety of activities online, including disrupting foreign threats to Canada.

The Minister of Foreign Affairs plays an important role to ensure FCO activities are in line with Canada's foreign policy. They must request or consent to any ACO Authorizations and be consulted before any DCO Authorizations can be issued.

The number of Ministerial Authorizations for ACO and DCO each calendar year since the *CSE Act* came into force was as follows:

- 2022:  
→ ACO: 3  
→ DCO: 1
- 2021:  
→ ACO: 2  
→ DCO: 1
- 2020:  
→ ACO: 1  
→ DCO: 1
- 2019:  
→ ACO: 1  
→ DCO: 1

Each authorization is valid for up to a year. CSE may carry out multiple operations under a single authorization. In some cases, the authorization may be precautionary, with no operations taking place.

### Ministerial Orders

Under the *CSE Act*, the Minister of National Defence may use Ministerial Orders to designate people or organizations with whom CSE can work or share information. For example, for CSE to provide cyber security assistance to a non-federal institution, the Minister would have to designate that organization's cyber systems as being "of importance to the Government of Canada".

As of March 31, 2023, there were 5 Ministerial Orders in effect:

- 3 orders designating non-federal cyber systems as being of importance to the Government of Canada
- 1 order designating entities with whom CSE may share information relating to a Canadian or person in Canada if it is necessary to protect the information or systems of federal institutions or critical infrastructure
- 1 order designating entities with whom CSE may share Canadian identifying information, if it is essential for international affairs, defence or security

### National security review bodies

All CSE's activities are subject to external review by:

- the National Security and Intelligence Review Agency (NSIRA)
- the National Security and Intelligence Committee of Parliamentarians (NSICOP)

These review bodies play a crucial role on behalf of Canadians to ensure CSE's activities are lawful. We welcome their insights to help us improve our processes.

This year, CSE restructured its review coordination team to better support NSIRA reviews.

CSE continued to engage with NSIRA to address their concerns about accessing CSE information. Both parties agreed to a pilot solution that gives NSIRA independent access to CSE files related to NSIRA reviews. The pilot began in March 2023, and we continue to monitor and take feedback from NSIRA on this progress.

## Reviews of foreign interference

In March 2023, the Prime Minister announced measures to [strengthen trust in Canada's democracy](#).<sup>88</sup> This included requesting NSICOP and NSIRA to review the impact of foreign interference in the 2019 and 2021 federal elections, and how Canada's national security agencies handled the threat.

The Prime Minister also appointed an [Independent Special Rapporteur on Foreign Interference](#),<sup>89</sup> with a mandate to make interim recommendations by May 23, 2023.

In March, CSE began supporting the Independent Special Rapporteur by:

- providing briefings
- answering questions
- supplying classified and unclassified documents

NSIRA and NSICOP launched their reviews in March, with CSE receiving the first requests for information in April.

CSE supports these reviews. As we have outlined in reports such as [Cyber threats to Canada's democratic process](#),<sup>91</sup> the threat of foreign interference is real. Canadians need to be able to trust in the outcomes of elections.

## Review statistics

This fiscal year CSE:

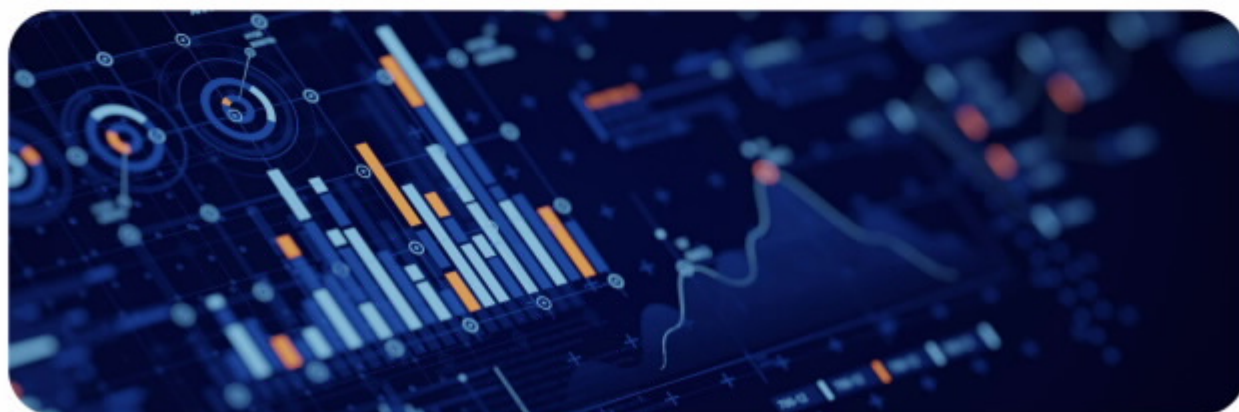
- contributed to 22 external reviews:
  - 17 by NSIRA
  - 4 by NSICOP
  - 1 by the Independent Special Rapporteur
- held 52 briefings, meetings or interviews with review staff
- responded to 502 questions from our review bodies

CSE answered 89% of questions submitted by NSICOP and NSIRA by the requested due date.

## Reports by our oversight and review bodies

Unclassified reports by our external oversight and review bodies can be found on their websites:

- [Intelligence Commissioner](#)<sup>92</sup>
- [NSICOP](#)<sup>93</sup>
- [NSIRA](#)<sup>94</sup>



## Accountability

### Protecting Canadian privacy

CSE follows strict protocols to make sure our activities comply with the law and respect the privacy of Canadians and people in Canada. Our activities are subject to review by external review bodies including the Privacy Commissioner.

Learn more about how [CSE protects privacy](#)<sup>95</sup> on our website.

#### Metadata sharing

In January 2023, CSE resumed sharing metadata with our Five Eyes partners after an extensive, multi-year process to address privacy concerns.

Metadata refers to information **about** a communication but not the content of the communication itself. Examples of metadata include:

- the date and time of a communication
- email addresses
- IP addresses
- phone numbers

Metadata is an essential part of foreign intelligence tradecraft, helping analysts to identify who a target is communicating with, when and how. This valuable context helps the Government of Canada, and our Five Eyes allies to respond appropriately to foreign-based threats.



#### Metadata and Canadian Identifying Information

CSE gathers metadata under the foreign intelligence aspect of our mandate, which prohibits us from targeting the communications of Canadians or anyone in Canada. However, the global information infrastructure (GII) is just that – global. Therefore, when acquiring information from the GII, CSE may incidentally acquire information that can be used to identify a Canadian or person in Canada.

Learn more about how [CSE protects Canadian Identifying Information \(CII\)](#).<sup>96</sup>

Prior to 2014, CSE used an automated process to “minimize” CII (make it unidentifiable) before sharing metadata with Five Eyes partners.

However, in 2014, CSE discovered that the automated process was not minimizing CII properly. We immediately suspended metadata sharing and informed the Office of the Privacy Commissioner and the CSE Commissioner, our external review body at the time.

The Chief of CSE and the Minister of National Defence made a commitment that CSE would not resume metadata sharing until effective measures to protect Canadians’ privacy were in place.



### Query-in-place

To address this issue, CSE has instead adopted a new process to allow our Five Eyes partners to use CSE acquired metadata. The process is called “query-in-place” (QIP) because the overall database does not leave CSE’s control. Instead, analysts at partner agencies may submit a query to CSE for specific data. These requests:

- must **not** be directed at a Canadian or anyone in Canada
- must clearly state who or what is the target of the query
- must clearly state the information the query is intended to return and its foreign intelligence value

Compliance with these requirements is monitored by CSE. All Five Eyes analysts who wish to submit queries through QIP must first complete mandatory training and a knowledge test on CSE’s legal and policy requirements.

### Consultation

Before launching QIP, CSE went through an extensive consultation process. We briefed the Minister of National Defence and the National Security and Intelligence Review Agency (NSIRA). We worked closely with the Office of the Privacy Commissioner (OPC) to identify and address privacy risks and to introduce technical measures to reduce them.

As per the OPC’s recommendation, CSE conducted a Privacy Impact Assessment (PIA) on our metadata sharing process. Because the PIA contains Top Secret information, we held multiple in-person briefings for the OPC so that classified details could be discussed in full.

The OPC made 6 recommendations to explain certain concepts in the PIA more clearly, all of which CSE accepted.

### Sharing

CSE ran a pilot of query-in-place from November 2021 to December 2022, which resulted in 0 privacy incidents.

Having verified that the process was working as it should, CSE notified our Five Eyes partners in January 2023, that the pilot phase was concluded, and that QIP will be the new standard of sharing CSE metadata.

CSE continues to conduct compliance checks to ensure continued compliance with CSE’s legal and policy requirements.

With QIP, CSE has resumed a valuable contribution to the Five Eyes: an alliance that shares Canada’s democratic values and that helps to protect our interests in the world.

### Disclosures of Canadian Identifying Information

As mentioned, CSE’s foreign intelligence activities do not target the communications of Canadians or anyone in Canada. When Canadian Identifying Information (CII) gets acquired incidentally, CSE obfuscates the CII in our intelligence reporting.

However, under the *Privacy Act*, a limited number of clients who receive CSE’s classified intelligence reports can request the details of the CII, as long as they have both the legal authority and an operational need to know. For example, this could include the role of a “named Canadian” in activities that raise national security concerns. Disclosures of CII may be reviewed by NSIRA.

In 2022, CSE received:

- 719 requests to disclose CII
  - 657 from GC partners
  - 62 from Five Eyes partners

Of these requests, CSE:

- approved: 530
- denied: 65

The balance were either cancelled or still in process as of December 31, 2022.

## Accountability

### Operational privacy incidents

CSE has detailed internal policies on how to handle information related to Canadians. Any occurrence, however minor, that runs counter to these policies is considered an operational privacy incident. This is an internal tracking mechanism. It includes minor procedural errors (such as mislabelled data) that do not meet the threshold for reporting to the Privacy Commissioner.<sup>97</sup> Second party privacy incidents are counted separately. These are incidents that involve a Five Eyes agency.

In 2022, CSE internally tracked:

- 114 operational privacy incidents
- 23 second party privacy incidents

When an operational privacy incident is identified, CSE takes steps to correct the error, for instance by deleting data. CSE logs and tracks privacy incidents so we can take steps to prevent future incidents. Actions include updating our policies or retraining employees.

### Internal compliance

In addition to external oversight and review, CSE also has a rigorous internal compliance program to make sure our activities comply with the law and protect Canadian privacy. The compliance team verifies CSE's operational activities and educates CSE employees on compliance.

This fiscal year, CSE's compliance team conducted:

- 17 reviews
- 8 studies
- 2 spot checks

Any CSE employee who needs to access raw data to do their work must undergo annual compliance training and knowledge testing. If they fail, their access to those systems is revoked and they must re-train.

We also encourage CSE analysts to report any potential privacy incidents. The vast majority of CSE's internal compliance incidents are self-reported.

In November 2022, CSE held its first annual Operational Compliance Week. This included a mix of formal and informal activities to raise awareness and share best practices.



### Complaints

Members of the public may [file a complaint](#)<sup>98</sup> about CSE's activities by writing to the Chief of CSE. If the complainant is not satisfied by our response, they may refer their complaint to NSIRA. NSIRA will then investigate to determine whether or not the complaint falls within their jurisdiction.

This fiscal year, CSE received:

- 8 external complaints, of which:
  - 4 complaints were investigated and closed
  - 4 complaint investigations were in various stages of completion (as of March 31, 2023)

This year CSE and NSIRA worked together to develop a process for NSIRA to view CSE's findings relating to complaints. The new process is intended to improve transparency, making it easier for NSIRA to determine whether or not a complaint falls within their jurisdiction. It was used for the first time in January 2023.



## Transparency

It is essential for our democracy that Canadians understand what CSE does to protect our national security. At the same time, some information is too sensitive to release because adversaries could use it to harm us.

CSE is committed to working with review bodies, external partners, media outlets and Canadians to promote transparency about our activities as part of the [National Security Transparency Commitment](#).<sup>99</sup>

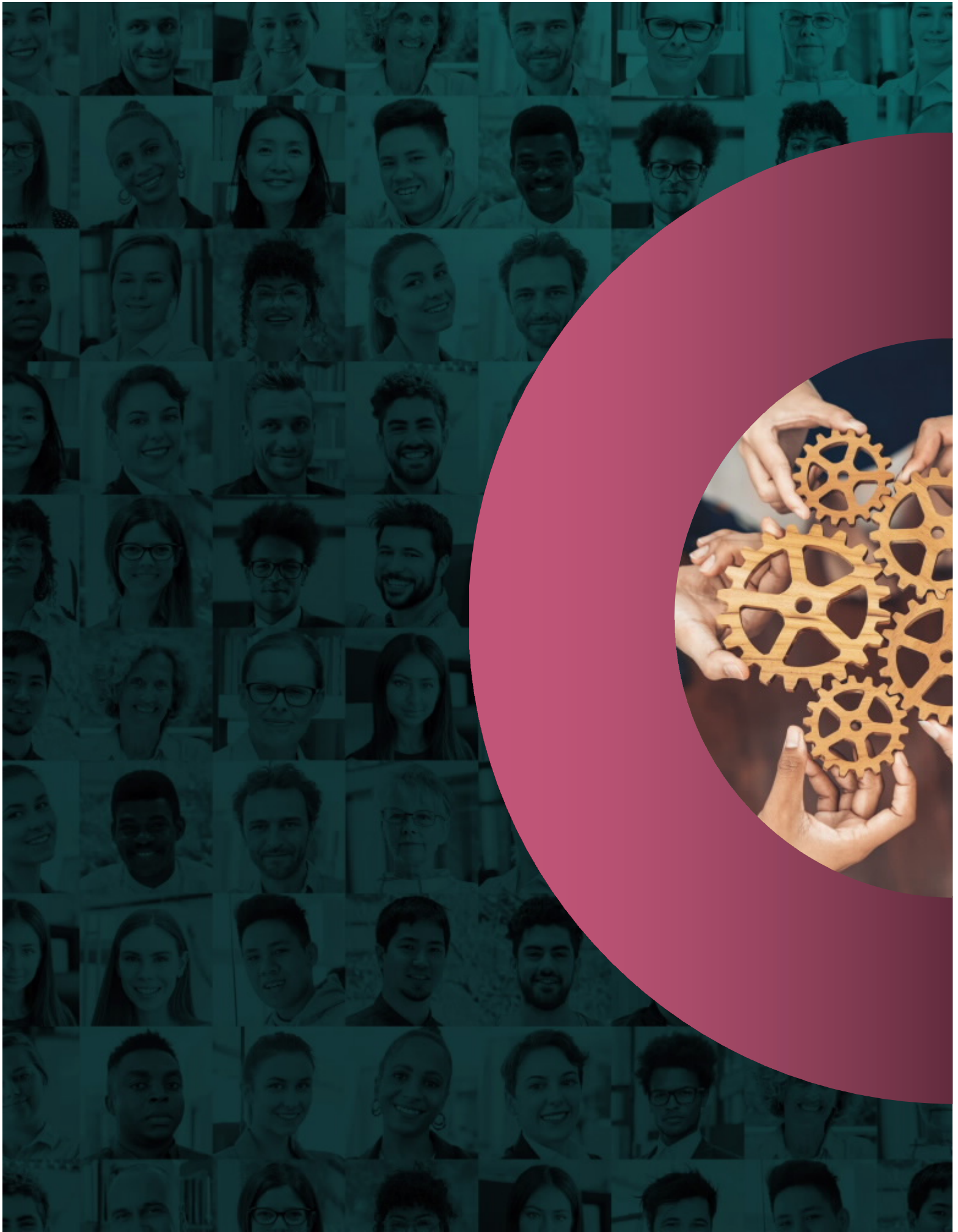
The National Security Transparency Advisory Group (NS-TAG) advises government officials on how to strike the balance between transparency and security concerns. In October 2022, Chief Caroline Xavier briefed NS-TAG on CSE's activities and answered questions about CSE's:

- data retention policies
- assistance to critical infrastructure
- technical and operational assistance to federal partners

This year, CSE's transparency activities included:

- 4 [public reports](#)<sup>100</sup>
- 4 [proactive disclosures](#)<sup>101</sup>
- 11 parliamentary appearances
- 14 media interviews
- 34 [Open Government](#)<sup>102</sup> releases
- 53 [Access to Information](#)<sup>103</sup> responses
- multiple speeches, conferences and public events

We also leveraged digital tools like the CSE website and our social media accounts to communicate our activities to a greater number of Canadians and increase their awareness of our work.



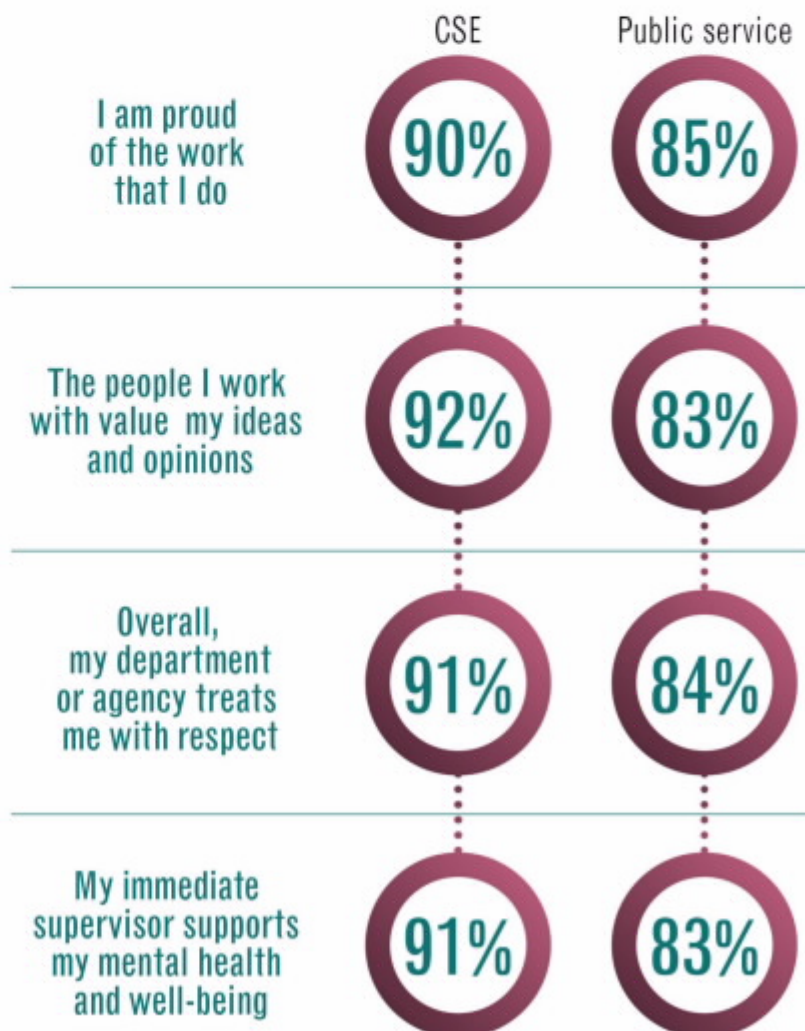
## People

CSE employees come from a variety of backgrounds and bring their diverse experiences and knowledge to work towards one common goal: protecting Canada and Canadians.

When our people feel supported in their work and their identities, CSE is better able to deliver on our mission. Over the past year, we've increased our efforts to foster a healthy and inclusive environment to support our existing employees and help attract new ones.

### Employee survey results

The Public Service Employee Survey (PSES) gathers data from public servants about their experiences in the workplace. [CSE's 2022 PSES results<sup>104</sup>](#) were consistently better than the public service average. For example:



## People

However, there is always room for improvement. For example, the percentage of CSE employees who experienced harassment or discrimination, while low, is not what it should be (zero), and has increased slightly since 2020:

- harassment:
  - 2022: 8%
  - 2020: 6%
- discrimination
  - 2022: 6%
  - 2020: 5%

The percentage of CSE employees reporting work-related stress has gone down since 2020 but is still higher than it was before the pandemic:

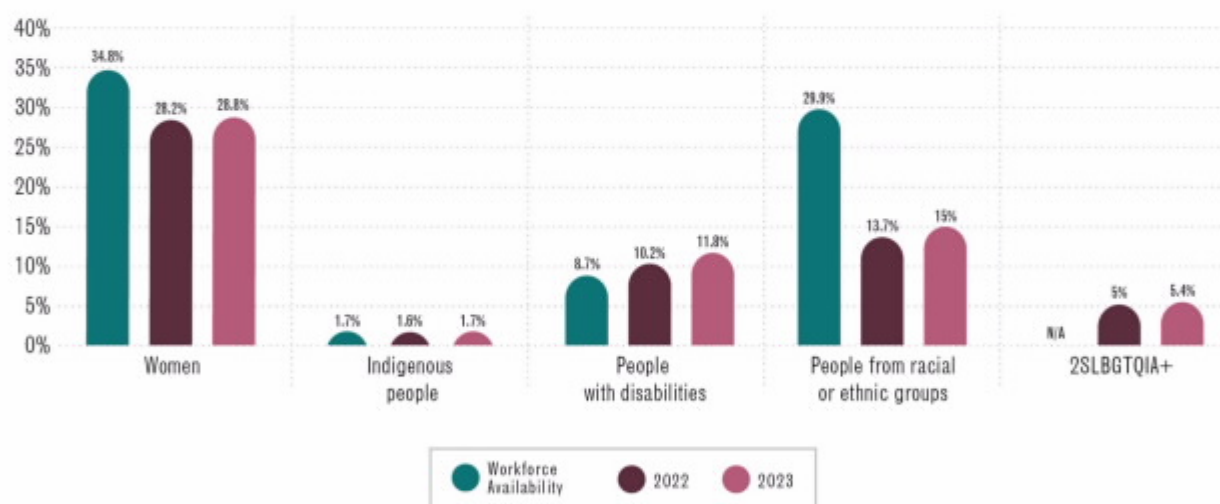
- high or very high work-related stress:
  - 2022: 13%
  - 2020: 15%
  - 2019: 9%

The first principle of [CSE's EDI framework](#)<sup>105</sup>, is “CSE is a work in progress”. We are always striving to do better. The 2022 PSES data provides invaluable feedback to help us identify areas where change is needed.

## Demographics

In 2022, CSE adopted a new process for gathering data on workforce demographics and employment equity representation. This included updated definitions, and a new option to self-identify as a member of the 2SLGBTQIA+ community. To date 75% of CSE employees have chosen to submit voluntary self-identification data.

### Workforce demographics at CSE 2022 to 2023



Our latest numbers show that diversity is slowly increasing at CSE. Our representation of Indigenous employees and employees with disabilities is now equal to or higher than their workforce availability. However, women and employees from racial or ethnic groups remain underrepresented. This is something we are determined to change, in accordance with the [Call to Action on Anti-Racism in the Federal Public Service](#)<sup>106</sup> and the CSE EDI framework. We continue to work with internal and external partners to improve in these areas, notably through tailored recruitment, future of work initiatives and efforts to promote EDI.

## Recruitment

As mentioned, Budget 2022 allocated new funds for CSE to expand our capacities. This meant that growth was top of mind for us this year. We undertook several initiatives to improve our ability to attract and hire the people we need to effectively carry out our mission and fulfill growing demands.

### Recruitment events

CSE's Candidate Outreach team adopted a hybrid approach, attending a mix of both in person and online recruitment events. They participated in 90 events such as career fairs in colleges and universities, hackathons, information sessions and technical workshops. To support our efforts to recruit a more diverse workforce, nearly a quarter of these events catered specifically to jobseekers from underrepresented communities.

### Recruiting Indigenous employees

As we work towards reconciliation, CSE is committed to addressing employment gaps experienced by Indigenous Peoples and ensuring they have equitable access to opportunities. This year, CSE attended recruitment fairs in cities with large Indigenous populations and has been working closely with an internal Indigenous subject matter expert to further our reach in these communities.

CSE continued to participate in the Government of Canada's [IT Apprenticeship Program for Indigenous Peoples](#).<sup>107</sup> This program matches First Nations, Inuit, and Métis candidates with participating organizations to help them build the skills they need for an IT career in the federal public service.

We consulted our [affinity groups](#)<sup>108</sup> to identify systemic inequities in our hiring practices. Of note was the relocation requirement which presented a barrier for Indigenous candidates whose identities are deeply tied to their communities. With our new hybrid work model, Indigenous candidates wishing to remain in their communities can request to work remotely if their position allows for it (see [Future of work](#) on p.54).

### Recruitment marketing

In spring 2022, CSE completed an advertisement campaign to recruit foreign language intelligence analysts specializing in Chinese languages. The campaign ran in Chinese-language media to reach Canadians with Chinese language skills. This campaign generated more than 2,500 visits to our career webpage.

In December 2022, CSE released a [new recruitment video](#)<sup>109</sup> highlighting the various types of jobs available at CSE and showcasing the elements of our culture that make us who we are. The video was created entirely in-house and was accompanied by new branding and a new slogan: "CSE – The most important organization you've never heard of".

### Other recruitment efforts

For the first time in 3 years, CSE published a dedicated intelligence analyst poster on our careers page. It received over 1,900 eligible applicants.

We continued to engage with current and future tech talent through collaborative events, such as GeekWeek, and our community outreach program.





## Security

A large part of our hiring process involves a security assessment. This is necessary because our work affects Canada's national security. However, we are aware that this process can be daunting, especially for candidates belonging to groups that experience discrimination.

This year, CSE's security team consulted affinity groups to identify barriers that may discourage members of underrepresented groups from applying. Together, they have been exploring ways to make our screening process more inclusive, such as:

- increasing cultural awareness and knowledge of unconscious biases among security officers
- working to increase the diversity of CSE's security personnel, both through external and internal recruitment

## Future of work

As mentioned in last year's report, CSE has embraced the multi-classification and hybrid environment brought on by the pandemic. This has allowed us to offer more flexibility to our employees and expand our security classifications.

### Hybrid workplace

The telework pilot we launched last year was a great success. CSE has now formally adopted a hybrid work model. Our strategy is adapted from the [federal public service's hybrid work model](#)<sup>111</sup> and sees the majority of our employees working onsite at least 3 days each week.

To support a fair, equitable and sustainable approach, we've set out considerations for those requesting additional days offsite. With the appropriate approvals, exceptions can be made for situations such as:

- employees working across Canada
- Indigenous employees wishing to remain in their communities
- employees in priority IT areas

That said, employees whose work is classified continue to work onsite full time. This was the case throughout the pandemic and has continued with the shift to hybrid.

Our priority remains to carry out our mission efficiently, while supporting our workforce through flexible work arrangements.



## Enhanced reliability status

Our hybrid work model has shown us that we can maintain the same level of efficiency and excellence in a multi-classification environment. We have taken this as an opportunity to expand our security classifications to bring in more people, more quickly.

This year we implemented an **enhanced reliability status (ERS)** for roles that do not require access to our classified systems and information. Features of the program include:

- quicker security screening – security interviews may be conducted remotely and polygraphs are not required
- expanded pool of candidates – employees based outside the National Capital Region may work remotely
- career pathways allow for advancement without the need for a top-secret clearance

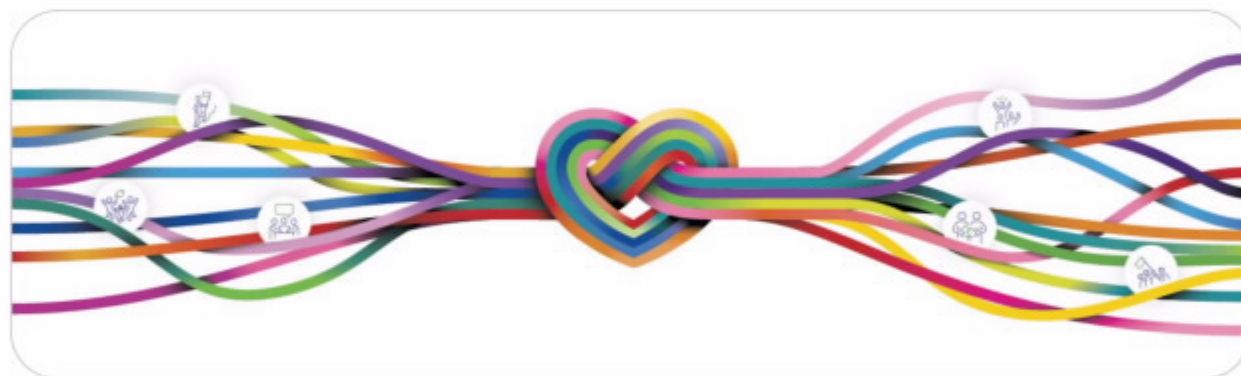
Since the ERS was implemented in July 2022, 17 full-time permanent employees and 10 students have been hired through the program. CSE will continue to leverage the ERS over the coming years to meet our growth goals.

## Equity, diversity and inclusion (EDI)

CSE is committed to building a workforce that's as diverse as it can be. We strive to foster an inclusive and equitable environment where all employees can thrive. This isn't just important for our workplace culture, it's essential to our mission.

Through internal and external collaborations, we're taking steps to raise awareness, identify systemic inequities and find solutions to improve the experiences of everyone at CSE.

To read more about other EDI initiatives, visit the [diversity and inclusion section](#)<sup>112</sup> of our website.



## EDI framework

In June 2022, we launched the [CSE EDI Framework](#).<sup>113</sup> Over the past year, we have used the framework to:

- guide our efforts to create a more inclusive organization
- promote EDI at all levels and in all activity areas
- ensure the right people are at the right tables
- bolster the effectiveness of our mission

This year, every activity area at CSE developed a yearly EDI action plan that takes the elements laid out in the framework and turns them into concrete tailored action. Representatives from each area will work together to ensure accountability and report on progress made.

## People

### Sponsorship pilot program

In December 2022, CSE launched a sponsorship pilot program. This program was developed to:

- eliminate barriers to advancement experienced by Black, Indigenous and other racialized employees
- provide Black, Indigenous and other racialized employees with opportunities to help them advance their careers
- create equitable career progression processes at CSE

It aims to do so by matching participants with senior sponsors (CSE executives) who will:

- coach, champion and invest in them
- ensure that they are actively considered for opportunities
- help them secure a suitable acting appointment

The pilot received 56 applications. Of those, 14 candidates were chosen to take part in this program for 12 months starting in April 2023. Candidates who were not selected in this first round were offered access to career support and informal mentorship opportunities.

The sponsorship program is evidence that CSE is putting in the effort to tackle some of the systemic barriers faced by racialized and Indigenous employees. It shows that CSE is not afraid of being a leader of change. As a racialized woman, I'm very aware of the inequities that many may face in the workplace and I'm glad CSE is taking the necessary steps to combat these.

Sabeena S. (she/her), CSE employee and sponsorship program participant



### CSE's Accessibility Plan 2022-2025

The very first [CSE Accessibility Plan](#)<sup>114</sup> was published in December 2022. The plan presents an overview of the actions we have taken and intend to take to remove barriers to accessibility for employees and visitors. It was created in consultation with various internal groups, including:

- affinity groups (including the disability and neurodiversity groups)
- union representatives
- [People Committee](#)<sup>115</sup>

Over the next 3 years, we will work together to refine the plan and ensure that no one is left behind. We've also established a process for [providing feedback on accessibility at CSE](#).<sup>116</sup>

## Affinity groups

CSE's [affinity groups](#)<sup>117</sup> are employee-led networks that play a key role in the implementation of the CSE EDI framework. As of 2023, they're also important members of our People Committee, where they sit on a rotational basis to provide diverse perspectives.

This year, CSE employees launched 2 new affinity groups:

- Jewish Affinity Group
- Réseau franco

Throughout the year, our affinity groups helped develop policies and led initiatives that benefit people at CSE, including:

- the CSE EDI Framework
- the CSE Accessibility Plan 2022-2025
- our internal guide on supporting neurodiversity at CSE
- a structured mentorship program with over 100 participants

They also organized many [events and commemorations](#) (see p.58), advocated for the needs of their communities and shared their lived experiences.

In January 2023, EmBRACE (our network for Indigenous and racialized employees) organized a visit from their GCHQ counterparts to strengthen our partnership in the EDI space. Read more about this [historic visit to promote anti-racism at CSE and GCHQ](#).<sup>118</sup>

## EDI training

One of the key principles of the CSE EDI Framework is that CSE learns. To support this, the framework outlines the need for implementing mandatory training on Gender Based Analysis Plus and relevant topics related to EDI.

This year, CSE mandated the following trainings:

- For all employees
  - Introduction to Gender-Based Analysis Plus (GBA Plus)
  - Moving from bias to inclusion
- For supervisors and managers
  - Leading Diversity
  - Adopting an Inclusive Mindset at Work

We also provided several other informal trainings that addressed topics like microaggressions and gender identity and expression.

## Senior Advisor for People, Equity, Diversity and Inclusion

CSE welcomed a new Senior Advisor to the Chief on Equity, Diversity and Inclusion this year. They helped build EDI into the organization in a more sustainable way by championing changes including:

- launching the sponsorship pilot program
- changing the structure of People Committee to include affinity group leads
- providing corporate support to the affinity groups
- improving data collection and use of data to support EDI at CSE



## People

### Award-winning anti-racism advocates

Over the past year, CSE employees Marie Calixte-McKenzie and Jonathan Gohidé continued to talk candidly about their experiences as Black people in Canada to audiences across the public service and beyond. They gave 11 presentations in both official languages, reaching over 1,000 people. A recording of their [Being Black in Canada presentation](#)<sup>119</sup> was also shown to all new employees as part of CSE's onboarding curriculum.

In October 2022, Marie and Jonathan were awarded the [2021 Joan Atkinson Award for Public Sector Values in the Workplace](#)<sup>120</sup> at the 2021 Public Service Awards of Excellence. These are the highest awards available to recognize outstanding contributions made by public servants.



### EDI events and commemorations

Throughout the year, CSE hosted over 25 events to raise awareness of various EDI topics. Many of these were organized by our affinity groups to educate their peers and commemorate important dates. Some joint events presented opportunities to collaborate with our Five Eyes partners in the EDI space.

# 13

In-person  
special events



Inuit throat singing duo, Tarniriik, performs at CSE to mark National Indigenous Peoples Day

# 10

Employee panel  
conversations



Informational material to promote International Women's Day at CSE

# 5

Guest speaker  
events



Eva Kuper, Holocaust survivor, speaks at CSE's International Holocaust Remembrance Day commemoration

## Official languages

CSE continued to promote linguistic duality at all levels and in all areas of the organization this year. In November 2022, CSE launched our Official Languages Action Plan which aims to address 2 main objectives:

- Create an inclusive bilingual workplace by increasing the use of French
- Ensure CSE has sufficient bilingual capacity to effectively execute public-facing programs and services for Canadians in both languages

We supported employees through formal part-time and full-time second-language training and promoted informal learning opportunities. New this year, CSE volunteers offered weekly French conversation groups for those looking to improve or maintain their French proficiency.

In March 2023, CSE welcomed the launch of the Réseau franco, a new affinity group that represents the needs and interests of CSE's francophone community. The Réseau franco hosted a week of events during the Semaine de la Francophonie to celebrate and promote the French language and francophone cultures.

## Employee wellbeing

The work we do can be demanding. CSE's focus on employee mental health and wellbeing ensures our people are emotionally resilient and have access to the resources they need when they need them.

Our Employees and Organization Wellness program (EOW) is made up of our:

- Counselling and Advisory Program (CAP)
- Career Services
- Disability Management Program

This year, CSE's in-house CAP directed its efforts towards the following activities:

- Engaging in an organization-wide consultation related to mental health to inform the development of a multi-year CSE mental health strategy
- Developing mandatory training for leaders on mental health, conflict management, and giving and receiving feedback
- Providing support for reintegration in a hybrid work environment
- Offering just-in-time support around conflict management and mental health

Our [Focus on employees page](#)<sup>121</sup> provides more information about the EOW program and its associated services.



## A greener CSE

Our Greener CSE program was hard at work this year providing environmental guidance on corporate projects and educating staff on various environmental issues.

For example, in June 2022 they led the installation of a beehive outside CSE's Edward Drake Building.

By the fall, our small but mighty beehive housed approximately 40,000 bees who produced 125 jars of unpasteurized wildflower honey and helped our local flora thrive.

## Awards

CSE was proud to be recognized once again as one of [Canada's Top Employers for Young People](#)<sup>122</sup> (2023) and named one of the [National Capital Region's Top Employers](#)<sup>123</sup> (2023).

This year, we were also awarded the [2022 Government of Canada Workplace Charitable Campaign Chair's Cup - Large Organization](#).<sup>124</sup> The Chair's Cup recognized the success of our charitable campaign which aims to support local communities.

CSE works hard to be an employer of choice because attracting and retaining top talent is the key to delivering our mission for Canadians.

If you've read this far,  
maybe you'd like to  
**come work with us!**<sup>125</sup>



## Endnotes

- 1 [cyber.gc.ca/en/](https://www.cyber.gc.ca/en/)
- 2 [laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html](https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html)
- 3 [www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 4 [www.budget.canada.ca/2022/report-rapport/chap5-en.html#2022-1](https://www.budget.canada.ca/2022/report-rapport/chap5-en.html#2022-1)
- 5 [www.youtube.com/watch?v=GyiPpqRd-Fw](https://www.youtube.com/watch?v=GyiPpqRd-Fw)
- 6 The Budget 2022 document lists \$263.9 million over 5 years and \$96.5 million ongoing, which represents accrual funding. CSE reports funding on a cash basis, in other words, the amount received.
- 7 [www.international.gc.ca/world-monde/issues\\_development-enjeux\\_developpement/peace\\_security-paix\\_secureite/cyberspace\\_law-cyberespace\\_droit.aspx?lang=eng](https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_secureite/cyberspace_law-cyberespace_droit.aspx?lang=eng)
- 8 [www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2021-2022](https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2021-2022)
- 9 [twitter.com/cse\\_cst/status/1509872778144632842](https://twitter.com/cse_cst/status/1509872778144632842)
- 10 [www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-russian-state-sponsored-and-criminal-cyber-threats-critical](https://www.cyber.gc.ca/en/news-events/joint-cyber-security-advisory-russian-state-sponsored-and-criminal-cyber-threats-critical)
- 11 [www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine](https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-activity-related-russian-invasion-ukraine)
- 12 [www.cyber.gc.ca/en/guidance/cyber-security-guidance-heightened-threat-levels-itsap10101](https://www.cyber.gc.ca/en/guidance/cyber-security-guidance-heightened-threat-levels-itsap10101)
- 13 [www.cyber.gc.ca/en/alerts-advisories/risk-malicious-cyber-activity-against-ukraine-aligned-nations](https://www.cyber.gc.ca/en/alerts-advisories/risk-malicious-cyber-activity-against-ukraine-aligned-nations)
- 14 [www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html](https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html)
- 15 [www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html](https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html)
- 16 [pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening](https://pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening)
- 17 [dgc-cgn.org/digital-governance-standards-institute-releases-draft-standards-for-vote-tabulators-and-electronic-poll-books-for-60-day-public-review/](https://dgc-cgn.org/digital-governance-standards-institute-releases-draft-standards-for-vote-tabulators-and-electronic-poll-books-for-60-day-public-review/)
- 18 [www.cyber.gc.ca/en/guidance/cyber-threats-elections](https://www.cyber.gc.ca/en/guidance/cyber-threats-elections)
- 19 [www.canada.ca/en/campaign/online-disinformation.html#q](https://www.canada.ca/en/campaign/online-disinformation.html#q)
- 20 [www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 21 [www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update](https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update)
- 22 [www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300](https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300)
- 23 [www.international.gc.ca/world-monde/issues\\_development-enjeux\\_developpement/peace\\_security-paix\\_secureite/cyberspace\\_law-cyberespace\\_droit.aspx?lang=eng](https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_secureite/cyberspace_law-cyberespace_droit.aspx?lang=eng)
- 24 [www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html](https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html)
- 25 [www.canada.ca/en/global-affairs/news/2022/09/statement-on-irans-malicious-cyber-activity-affecting-albania.html](https://www.canada.ca/en/global-affairs/news/2022/09/statement-on-irans-malicious-cyber-activity-affecting-albania.html)
- 26 [www.rcaanc-cirnac.gc.ca/eng/1562939617400/1562939658000](https://www.rcaanc-cirnac.gc.ca/eng/1562939617400/1562939658000)
- 27 [www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 28 [science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships](https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships)
- 29 [www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 30 [www.cyber.gc.ca/en/guidance/cyber-supply-chain-approach-assessing-risk-itsap10070](https://www.cyber.gc.ca/en/guidance/cyber-supply-chain-approach-assessing-risk-itsap10070)
- 31 [www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071](https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071)
- 32 [www.cyber.gc.ca/en/guidance/cyber-threat-supply-chains](https://www.cyber.gc.ca/en/guidance/cyber-threat-supply-chains)
- 33 [www.cyber.gc.ca/en/news-events/cs-es-evolved-security-review-program](https://www.cyber.gc.ca/en/news-events/cs-es-evolved-security-review-program)

## Endnotes

---

- 34 [cyber.gc.ca/en/tools-services/common-criteria](https://www.cyber.gc.ca/en/tools-services/common-criteria)
- 35 [cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp](https://www.cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp)
- 36 [www.cyber.gc.ca/en/news-events/nist-announces-post-quantum-cryptography-selections](https://www.cyber.gc.ca/en/news-events/nist-announces-post-quantum-cryptography-selections)
- 37 [www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111](https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111)
- 38 [www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018](https://www.cyber.gc.ca/en/guidance/guidance-becoming-cryptographically-agile-itsap40018)
- 39 [www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111](https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111)
- 40 [ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy](https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy)
- 41 [www.budget.canada.ca/2022/home-accueil-en.html](https://www.budget.canada.ca/2022/home-accueil-en.html)
- 42 The Budget 2022 document lists \$252.3 million over 5 years and \$61.7 million ongoing, which represents accrual funding. CSE reports funding on a cash basis, in other words, the amount received.
- 43 [www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf](https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf)
- 44 The Budget 2022 document references \$178.7 million over 5 years, starting in 2022 to 2023, and \$39.5 million ongoing, which includes amounts for Shared Services Canada.
- 45 The Budget 2022 document lists \$180.3 million over 5 years and \$40.6 million ongoing, which represents accrual funding. CSE reports funding on a cash basis, in other words, the amount received.
- 46 [cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 47 [www.cga.ca/cyber-security/](https://www.cga.ca/cyber-security/)
- 48 [www.ieso.ca/en/Sector-Participants/Cybersecurity/Sector-Services---Lighthouse](https://www.ieso.ca/en/Sector-Participants/Cybersecurity/Sector-Services---Lighthouse)
- 49 [www.publicsafety.gc.ca/cnt/ntnl-scrpt/cbr-scrpt/cbr-scrpt-tl/index-en.aspx](https://www.publicsafety.gc.ca/cnt/ntnl-scrpt/cbr-scrpt/cbr-scrpt-tl/index-en.aspx)
- 50 [cyber.gc.ca/en/glossary](https://www.cyber.gc.ca/en/glossary)
- 51 [www.cyber.gc.ca/en/incident-management](https://www.cyber.gc.ca/en/incident-management)
- 52 [cyber.gc.ca/en/tools-services/assemblyline](https://www.cyber.gc.ca/en/tools-services/assemblyline)
- 53 [www.cyber.gc.ca/en/guidance/security-considerations-industrial-control-systems-itsap00050](https://www.cyber.gc.ca/en/guidance/security-considerations-industrial-control-systems-itsap00050)
- 54 [busrides-trajetsenbus.cspc-efpc.gc.ca/en/ep-85-en](https://busrides-trajetsenbus.cspc-efpc.gc.ca/en/ep-85-en)
- 55 [www.getcybersafe.gc.ca/en](https://www.getcybersafe.gc.ca/en)
- 56 [www.getcybersafe.gc.ca/en/blogs/how-secure-your-online-financial-transactions](https://www.getcybersafe.gc.ca/en/blogs/how-secure-your-online-financial-transactions)
- 57 [www.getcybersafe.gc.ca/en/blogs/what-know-about-internet-cookies](https://www.getcybersafe.gc.ca/en/blogs/what-know-about-internet-cookies)
- 58 [www.getcybersafe.gc.ca/en/blogs/spot-signs-cattfish-dating-platforms](https://www.getcybersafe.gc.ca/en/blogs/spot-signs-cattfish-dating-platforms)
- 59 [www.getcybersafe.gc.ca/en/resources/what-do-if-you-are-victim-phishing-scam](https://www.getcybersafe.gc.ca/en/resources/what-do-if-you-are-victim-phishing-scam)
- 60 [www.getcybersafe.gc.ca/en/cyber-security-awareness-month](https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month)
- 61 [www.getcybersafe.gc.ca/en/resources/video-phishing-shanty-ruin-cyber-criminals-day](https://www.getcybersafe.gc.ca/en/resources/video-phishing-shanty-ruin-cyber-criminals-day)
- 62 [www.getcybersafe.gc.ca/en/phishing](https://www.getcybersafe.gc.ca/en/phishing)
- 63 [www.cyber.gc.ca/en/news-events/federal-partners-remind-canadian-consumers-be-vigilant-cyber-threats-black-friday-and-cyber-monday](https://www.cyber.gc.ca/en/news-events/federal-partners-remind-canadian-consumers-be-vigilant-cyber-threats-black-friday-and-cyber-monday)
- 64 [www.getcybersafe.gc.ca/en/blogs/top-12-scams-holidays](https://www.getcybersafe.gc.ca/en/blogs/top-12-scams-holidays)
- 65 [www.getcybersafe.gc.ca/en/blogs/adopt-meaningful-gaming-habits-holiday-season](https://www.getcybersafe.gc.ca/en/blogs/adopt-meaningful-gaming-habits-holiday-season)
- 66 [www.getcybersafe.gc.ca/en/resources/how-celebrate-unboxing-day](https://www.getcybersafe.gc.ca/en/resources/how-celebrate-unboxing-day)
- 67 [www.getcybersafe.gc.ca/en/blogs/investment-scams-whats-fraudsters-toolbox](https://www.getcybersafe.gc.ca/en/blogs/investment-scams-whats-fraudsters-toolbox)
- 68 [www.getcybersafe.gc.ca/en/blogs/spear-phishing](https://www.getcybersafe.gc.ca/en/blogs/spear-phishing)
- 69 [www.getcybersafe.gc.ca/en/blogs/service-scams-whats-fraudsters-toolbox](https://www.getcybersafe.gc.ca/en/blogs/service-scams-whats-fraudsters-toolbox)
- 70 [www.getcybersafe.gc.ca/en/blogs/phishing-whats-fraudsters-tacklebox](https://www.getcybersafe.gc.ca/en/blogs/phishing-whats-fraudsters-tacklebox)



- 71 [www.getcybersafe.gc.ca/en/resources/fraudsters-toolbox](http://www.getcybersafe.gc.ca/en/resources/fraudsters-toolbox)
- 72 [www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024](http://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024)
- 73 [cyber.gc.ca/en/guidance/national-cyber-threat-assessments](http://cyber.gc.ca/en/guidance/national-cyber-threat-assessments)
- 74 [www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment](http://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment)
- 75 [www.cyber.gc.ca/en](http://www.cyber.gc.ca/en)
- 76 [www.cyber.gc.ca/en/news-events/cybersci](http://www.cyber.gc.ca/en/news-events/cybersci)
- 77 [www.cyber.gc.ca/en/guidance/cyber-security-career-guide](http://www.cyber.gc.ca/en/guidance/cyber-security-career-guide)
- 78 [www.cyber.gc.ca/en/guidance/certifications-field-cyber-security](http://www.cyber.gc.ca/en/guidance/certifications-field-cyber-security)
- 79 [www.cyber.gc.ca/en/guidance/cyber-security-career-guide](http://www.cyber.gc.ca/en/guidance/cyber-security-career-guide)
- 80 <http://www.cse-cst.gc.ca/en/mission/tutte-institute-mathematics-and-computing>
- 81 [www.cse-cst.gc.ca/en/culture-and-community/research/uniform-manifold-approximation-and-projection-umap](http://www.cse-cst.gc.ca/en/culture-and-community/research/uniform-manifold-approximation-and-projection-umap)
- 82 [news.artnet.com/art-world/refik-anadol-moma-ai-unsupervised-2213039](https://news.artnet.com/art-world/refik-anadol-moma-ai-unsupervised-2213039)
- 83 [www.cse-cst.gc.ca/en/mission/applied-research](http://www.cse-cst.gc.ca/en/mission/applied-research)
- 84 [www.cyber.gc.ca/en/tools-services/assemblyline](http://www.cyber.gc.ca/en/tools-services/assemblyline)
- 85 <http://www.cse-cst.gc.ca/en/mission/vulnerability-research-centre>
- 86 [www.cse-cst.gc.ca/en/information-and-resources/announcements/cs-es-equities-management-framework](http://www.cse-cst.gc.ca/en/information-and-resources/announcements/cs-es-equities-management-framework)
- 87 [www.canada.ca/en/intelligence-commissioner/annualreport.html](http://www.canada.ca/en/intelligence-commissioner/annualreport.html)
- 88 [www.cse-cst.gc.ca/en/corporate-information/mandate](http://www.cse-cst.gc.ca/en/corporate-information/mandate)
- 89 [pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening](http://pm.gc.ca/en/news/news-releases/2023/03/06/taking-further-action-foreign-interference-and-strengthening)
- 90 [www.canada.ca/en/democratic-institutions/services/independent-special-rapporteur/terms-conditions.html](http://www.canada.ca/en/democratic-institutions/services/independent-special-rapporteur/terms-conditions.html)
- 91 [www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update](http://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-july-2021-update)
- 92 [www.canada.ca/en/intelligence-commissioner.html](http://www.canada.ca/en/intelligence-commissioner.html)
- 93 [www.nsicop-cpsnr.ca/index-en.html](http://www.nsicop-cpsnr.ca/index-en.html)
- 94 [nsira-ossnr.gc.ca/](http://nsira-ossnr.gc.ca/)
- 95 [www.cse-cst.gc.ca/en/accountability/privacy](http://www.cse-cst.gc.ca/en/accountability/privacy)
- 96 [www.cse-cst.gc.ca/en/information-and-resources/fact-sheets/protecting-canadian-identifying-information-cses-foreign#DCSESI](http://www.cse-cst.gc.ca/en/information-and-resources/fact-sheets/protecting-canadian-identifying-information-cses-foreign#DCSESI)
- 97 Prior to this fiscal year, CSE maintained a separate Minor Procedural Errors File (MPEF). As of 2022, procedural errors are now included in the Privacy Incidents File (PIF).
- 98 [www.cse-cst.gc.ca/en/accountability/oversight#MAC](http://www.cse-cst.gc.ca/en/accountability/oversight#MAC)
- 99 [www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html](http://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html)
- 100 [www.cse-cst.gc.ca/en/accountability/transparency/reports](http://www.cse-cst.gc.ca/en/accountability/transparency/reports)
- 101 [www.cse-cst.gc.ca/en/accountability/transparency/proactive-disclosure](http://www.cse-cst.gc.ca/en/accountability/transparency/proactive-disclosure)
- 102 [open.canada.ca/en](http://open.canada.ca/en)
- 103 [www.cse-cst.gc.ca/en/accountability/transparency/access-information-and-privacy-atip](http://www.cse-cst.gc.ca/en/accountability/transparency/access-information-and-privacy-atip)
- 104 [www.tbs-sct.canada.ca/pses-saff/2022/results-resultats/en/bq-pq/index/89](http://www.tbs-sct.canada.ca/pses-saff/2022/results-resultats/en/bq-pq/index/89)
- 105 [www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion](http://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion)
- 106 [www.canada.ca/en/privy-council/corporate/about-call-action.html](http://www.canada.ca/en/privy-council/corporate/about-call-action.html)
- 107 [talent.canada.ca/en/indigenous-it-apprentice](http://talent.canada.ca/en/indigenous-it-apprentice)
- 108 [www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/affinity-groups](http://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/affinity-groups)
- 109 [youtu.be/GyiPpqRd-Fw](https://youtu.be/GyiPpqRd-Fw)

## Endnotes

---

- 110 [www.cse-cst.gc.ca/en/careers](http://www.cse-cst.gc.ca/en/careers)
- 111 [www.canada.ca/en/government/publicservice/staffing/common-hybrid-work-model-federal-public-service.html](http://www.canada.ca/en/government/publicservice/staffing/common-hybrid-work-model-federal-public-service.html)
- 112 [www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion](http://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion)
- 113 [www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion](http://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion)
- 114 [cse-cst.gc.ca/en/accessibility/cse-accessibility-plan-2022-2025](http://cse-cst.gc.ca/en/accessibility/cse-accessibility-plan-2022-2025)
- 115 [cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion#pc](http://cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion#pc)
- 116 [cse-cst.gc.ca/en/accessibility/feedback-process-communications-security-establishment](http://cse-cst.gc.ca/en/accessibility/feedback-process-communications-security-establishment)
- 117 [www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/affinity-groups](http://www.cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/affinity-groups)
- 118 [www.cse-cst.gc.ca/en/information-and-resources/news/historic-visit-promote-anti-racism-cse-and-gchq](http://www.cse-cst.gc.ca/en/information-and-resources/news/historic-visit-promote-anti-racism-cse-and-gchq)
- 119 [www.cse-cst.gc.ca/en/being-black-canada-interview-cse-employees-jonathan-and-marie](http://www.cse-cst.gc.ca/en/being-black-canada-interview-cse-employees-jonathan-and-marie)
- 120 [www.canada.ca/en/treasury-board-secretariat/services/innovation/awards-recognition-special-events/psae-2021.html#toc-6](http://www.canada.ca/en/treasury-board-secretariat/services/innovation/awards-recognition-special-events/psae-2021.html#toc-6)
- 121 [www.cse-cst.gc.ca/en/culture-and-community/life-cse/focus-employees](http://www.cse-cst.gc.ca/en/culture-and-community/life-cse/focus-employees)
- 122 [reviews.canadastop100.com/top-employer-communications-security-establishment#young](http://reviews.canadastop100.com/top-employer-communications-security-establishment#young)
- 123 [reviews.canadastop100.com/top-employer-communications-security-establishment](http://reviews.canadastop100.com/top-employer-communications-security-establishment)
- 124 [www.canada.ca/en/campaign/charitable/gcwc-cc-appreciation-event/gcwc-cc-chairs-cup-awards.html](http://www.canada.ca/en/campaign/charitable/gcwc-cc-appreciation-event/gcwc-cc-chairs-cup-awards.html)
- 125 [cse-cst.gc.ca/en/careers](http://cse-cst.gc.ca/en/careers)



