Communications Security Establishment
Centre de la sécurité des télécommunications

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

Communications Security Establishment

ANNUAL REPORT

2021–2022

Communications Security Establishment
1929 Ogilvie Road,
Ottawa, ON K1J 8K6
cse-cst.gc.ca

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

Table of **contents**

About this **report**

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[1] (Cyber Centre), which is the federal government's operational lead for cyber security.

CSE's mandate is detailed in the *CSE Act*[2] and has 5 parts:

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

This report is an unclassified summary of CSE's activities from April 1, 2021 to March 31, 2022.

Unless otherwise noted, "this year" refers to the fiscal year, not the calendar year.

Foreword from the **Minister of National Defence**

Events around the world this year have underlined just how important the Communications Security Establishment's (CSE's) mandate is.

Global powers are behaving in increasingly hostile and irresponsible ways, including in cyber space. As we have seen with Russia's egregious invasion of Ukraine, the two often go hand in hand.

Foreign actors are promoting false narratives to obscure the truth, sow division and justify the unjustifiable. To chart these murky waters, the Government of Canada needs solid facts about our adversaries' actions, plans, and capabilities. CSE's foreign signals intelligence supplies those facts.

High-profile incidents around the world have shown how easily a cyber breach can disrupt the essential services people rely on. CSE's Canadian Centre for Cyber Security is defending Canada's federal institutions against these threats. At the same time, it is working with critical infrastructure providers and sharing unique resources with Canadians to improve Canada's overall cyber resilience.

In recognition of the increasing importance of CSE's mandate, the Government of Canada is making significant investments to support CSE's activities.

This includes investing in CSE's ability to launch foreign cyber operations to prevent and defend against cyber attacks. It also includes sponsoring classified research into cutting-edge technologies like quantum computing and artificial intelligence.

As the threats we face continue to evolve and proliferate, these investments will ensure CSE has the resources it needs to help protect Canadians and to support Canada's strategic priorities well into the future.

- The Honourable Anita Anand,
  Minister of National Defence

> Oversee the Communications Security Establishment to ensure that they are in a position to lead Canada's response to rapidly evolving cyber risks and threats, including through adequate resources and close cooperation with our allies.
>
> **Prime Minister Justin Trudeau**
> *Minister of National Defence Mandate Letter,*[3]
> *December 16, 2021*

Message from the **Chief and Associate Chief**

Well, that was quite a year.

Since CSE's last annual report, cyber threats have continued to increase in volume and variety. The trend to live and work online has persisted, along with the pandemic. Events around the world have shifted intelligence priorities and introduced new cyber threat scenarios.

CSE's mission[4] has never been more relevant:

- gathering vital foreign signals intelligence
- protecting important Canadian systems
- conducting active and defensive cyber operations
- sharing our expertise with federal national security, police and defence partners

In this report, you will find details of how CSE delivered our mission over the past fiscal year. Not all the details, of course. There are aspects of our work (tradecraft, techniques and intelligence) that must remain secret to be effective. However, this report goes further than before to demonstrate what we do and how we do it. Indeed, this year, CSE has taken unprecedented steps to be more open and transparent.

In recent months, we have declassified intelligence about Russia's brazen disinformation campaigns, and shared it with Canadians on social media. This is not something most would have imagined us doing even a short time ago. We have warned Canadian organizations about the tools and techniques used by Russian-backed cyber threat actors. We have continued to share sanitized cyber threat indicators gleaned from classified intelligence. We have continued to share insights from classified sources in public threat assessments.

CSE's Canadian Centre for Cyber Security has continued to work with industry and critical infrastructure to improve Canada's digital resilience. We have shared practical cyber security know-how with Canadians through Get Cyber Safe, Cyber Security Awareness Month and social media. An unprecedented array of CSE executives have participated in public events, industry panels, academic conferences, parliamentary committees and media interviews. And although we cannot share classified details in these public forums, CSE works with our external oversight and review bodies so that Canadians can be confident that we comply with the law and respect their privacy in everything we do.

This report details the concrete steps we have taken as a community to address systemic inequities and how we have celebrated diversity and inclusion as non-negotiable mission imperatives. We have had frank conversations about mistakes of the past. We have worked to remove barriers to equity in our programs and processes, and we have had many positive experiences together as a community.

Our workplace affinity groups (for example, representing Black, Indigenous, neurodiverse, 2SLGBTQIA+, Jewish, and women employees) have provided game-changing feedback on how to make CSE a better workplace for everyone. Their leadership and lived experiences have helped to guide CSE's new Equity, Diversity and Inclusion Framework[5], which our executive committee approved in March 2022. We are very proud of the leadership and partnership CSE has shown in the Canadian and allied security and intelligence community.

Finally, in 2021 we celebrated our 75th anniversary as Canada's national cryptologic agency. It was a time to recognize those who preceded us and on whose shoulders we stand, including the 9 Chiefs of CSE who have served since 1946. Today, as we turn the page on our milestone anniversary, there is no doubt that CSE's work will only become more relevant with each passing year.

- Shelly Bruce, Chief CSE #10
- Dan Rogers, Associate Chief

STAND
WITH
UKRAINE

Russia's invasion of **Ukraine**

On February 24, 2022, Russian forces invaded Ukraine.

CSE has supported Canada's response to this illegal invasion by using both our cyber security and foreign signals intelligence (SIGINT) mandates.

Responding to Russian cyber threats

In the weeks leading up to the invasion, the Cyber Centre issued two public advisories warning Canadian critical infrastructure organizations to bolster their defences against known Russian-backed cyber threat activity.[6]

These advisories were informed by CSE SIGINT and Cyber Centre operational knowledge as well as Russia's track record of using its cyber capabilities irresponsibly, such as:

- the SolarWinds[7] cyber compromise
- activity aimed at COVID-19 vaccine research[8]
- activity aimed at Georgia's democratic process[9]
- the NotPetya malware[10] attacks on government and critical infrastructure targets around the world

> We know that Russia has sophisticated cyber attack capacities. Not just misinformation, disinformation. But attacks on infrastructure, on systems, on individuals and companies that can be very disruptive. Fortunately, over the past years, the investments we've made in CSE, that has been extraordinary and world class in cyber capabilities, is part of how we defend against Russian cyber attacks or cyber foreign attacks in general.
>
> **Prime Minister Justin Trudeau**
> *Government of Canada press conference, March 3, 2022*

Before, and throughout the invasion, the Cyber Centre continued to track cyber threat activity in Canada and around the world and to share that information with Canadian critical infrastructure partners. That threat feed includes:

- indicators of compromise (digital details about malicious activity)
- threat mitigation advice
- confidential alerts about:
  - → new forms of malware
  - → tactics being used to target victims

We also continued to share cyber threat information with key partners in Ukraine.

Supporting Canada’s response to the invasion of Ukraine

CSE supported Canada’s response to Russia’s unjustifiable invasion of Ukraine by providing timely and relevant foreign signals intelligence reporting in response to a broad range of client requirements.

For example, we supported operations to repatriate Canadian diplomatic personnel from Ukraine by providing intelligence on potential risks affecting them.

We continued to provide technical and operational assistance to Operation UNIFIER, the Canadian Armed Forces mission in support of Ukraine. This included intelligence sharing and cyber security support.

Countering Russian disinformation

CSE tracked Russian-backed disinformation campaigns related to the war in Ukraine, such as:

- false narratives that only military targets were being attacked
- antisemitic, anti-LGBTQ+, anti-immigrant, and anti-globalist conspiracy theories
- false stories about Canadian forces committing war crimes
- disinformation about NATO allies
- false claims that the US established military-biological labs in Ukraine

CSE declassified key observations from our intelligence reporting in order to expose these false narratives publicly. In April 2022, CSE shared these examples with Canadians on social media, along with resources to help identify disinformation.

Attributions

CSE works with Global Affairs Canada and other federal and international partners to call out irresponsible behaviour in cyber space. CSE contributes to these attributions using both intelligence analysis and cyber security expertise.

In April 2021, Canada joined our allies in attributing the SolarWinds cyber compromise[11] to a Russian state-sponsored actor. The threat activity compromised thousands of networks around the world, by installing malware through program updates. The threat actor then targeted a subset of those victims for cyber-espionage purposes.

In July 2021, Canada joined our allies in identifying People’s Republic of China (PRC) state-backed actors as responsible for the “unprecedented and indiscriminate” exploitation of Microsoft exchange servers.[12] An estimated 400,000 servers were affected worldwide and used to steal intellectual property and vast quantities of personal information.

As mentioned above, in January and February 2022, the Cyber Centre joined our US and UK allies to warn[13] and remind[14] Canadian organizations about known Russian-backed cyber threats to critical infrastructure.

Foreign signals **intelligence**

As Canada's foreign signals intelligence agency, CSE intercepts and analyzes electronic communications and other foreign signals to inform the Government of Canada about the activities of foreign entities that seek to undermine Canada's national security and prosperity. (We are prohibited by law from targeting the communications of Canadians anywhere or anybody in Canada.) CSE SIGINT also supports government policy-making in defence, security and international affairs.

Foreign-based threats

This year, CSE reported on a range of foreign-based threats, including:

- activities of hostile states, including cyber threats
- cybercrime
- espionage directed against Canada, including economic espionage
- foreign interference and disinformation campaigns
- kidnappings of Canadians abroad
- terrorism and extremism, including ideologically motivated violent extremism (IMVE)
- threats to Canadians and Canadian forces abroad

This fiscal year, CSE supported Canadian military operations abroad, including Operations IMPACT, UNIFIER and REASSURANCE and provided intelligence and assistance to help protect our forces deployed abroad.

CSE foreign signals intelligence also assisted Global Affairs Canada and CAF with the operation to airlift Canadians out of Kabul after the Taliban retook Afghanistan in August 2021.

CSE foreign intelligence reporting 2021 to 2022

3,202
Reports

1,686
Clients

27
Departments and agencies

Assisting federal partners and military operations

This year, CSE continued to fulfil our mandate to provide technical and operational assistance to federal law enforcement, security and defence partners 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)

Working with international partners

Canada is a member of the Five Eyes, along with the US, the UK, Australia and New Zealand. Canada benefits greatly from this decades-old strategic alliance which entails a profound level of intelligence sharing and cooperation on matters of common concern. CSE works very closely with its Five Eyes counterparts on a broad range of defence, foreign affairs and security priorities and the intelligence gained through these partnerships is of great benefit to the Government of Canada. CSE also maintains collaborative relationships with numerous SIGINT and cyber defence counterparts around the world.

CSE, together with our allies, promotes and respects norms of responsible behaviour in cyberspace, and we have called out actors who have violated these norms (see Attributions).

> Russia, China, and Iran are very likely responsible for most of the foreign state-sponsored cyber threat activity against democratic processes worldwide
>
> **Canadian Centre for Cyber Security**
> *Cyber Threats to Canada's Democratic Process: July 2021 update*[15]

Monitoring threats to Canada's democratic processes

CSE signals intelligence contributed to threat assessments, including the Cyber Centre's July 2021 update on cyber threats to Canada's democratic processes.

The report concluded that while Canada is a lower-priority target relative to other countries, it was still "very likely that Canadian voters (would) encounter some form of foreign cyber interference" ahead of and during the September 2021 federal election.

As a member of Canada's Security and Intelligence Threats to Elections (SITE) Task Force, CSE monitored potential threats to the 2021 General Election, in collaboration with SITE partners CSIS, RCMP and Global Affairs Canada. As part of this effort, CSE provided intelligence on the intentions, activities and capabilities of foreign threat actors.

In addition, CSE had cyber operations authorities in place to disrupt malicious cyber activity aimed at Elections Canada infrastructure, if needed (see Protecting democracy).

Meanwhile, the Cyber Centre worked with Elections Canada and the registered political parties to provide cyber security support (see Protecting democratic institutions).

Foreign cyber **operations**

Foreign cyber operations (FCO) are the newest part of CSE's mandate, dating back to the *CSE Act* in 2019. These authorities enable Canada to take action in cyberspace against foreign adversaries in matters relating to Canada's international affairs, defence or security.

Subdivided into defensive cyber operations (DCO) and active cyber operations (ACO), these authorities give Canada the option of acting on what CSE learns through our SIGINT and cyber security missions.

Under the *CSE Act*, these authorities must not:

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

The Minister of National Defence may only authorize ACO or DCO if they conclude that:

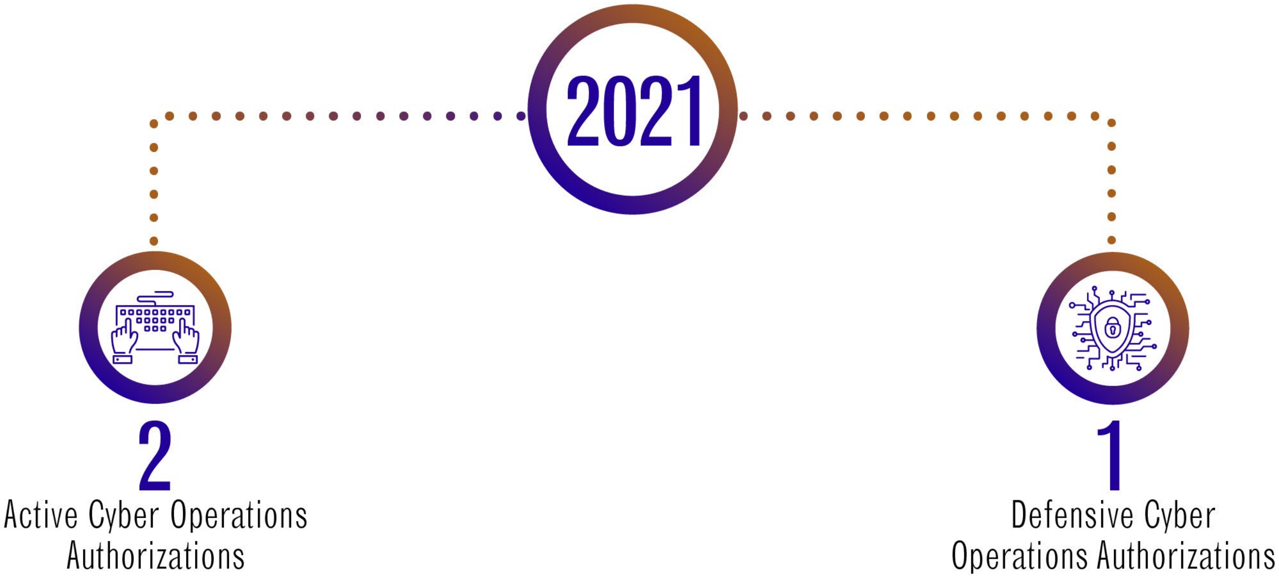
- the activities are reasonable
- the activities are proportionate
- the objective could not reasonably be achieved any other way
- no information will be acquired

The Minister of Global Affairs must consent to active cyber operations and must be consulted about defensive cyber operations.

Like all CSE's activities, foreign cyber operations are reviewed on behalf of Canadians by independent, external review bodies. These bodies produce public, unclassified reports of their findings. You can read more about how CSE cooperates with these review bodies in the Accountability section of this report.

Foreign cyber operations Authorizations

In 2021, the Minister of National Defence issued 3 Authorizations for foreign cyber operations.[16]



2021

2
Active Cyber Operations Authorizations

1
Defensive Cyber Operations Authorizations

Each Authorization is valid for up to one year. While multiple foreign operations may be conducted under a single Authorization, there are also cases where an Authorization may be anticipatory, with no operations required in the end. The DCO Authorization to protect the Canadian federal election is an example of this (see below).

Examples of foreign cyber operations

We can only share limited information about our foreign cyber operations in an unclassified report. However, in the interests of transparency, we have sanitized some examples of foreign cyber operations CSE has conducted or been authorized to conduct in the past. Due to sensitivities of discussing ongoing operations, these examples do not necessarily correspond to this fiscal year.

Disrupting foreign extremists

CSE has used its active cyber operations capabilities to disrupt the efforts of foreign-based extremists to:

- recruit Canadian nationals
- operate online
- disseminate violent extremist material

Countering cybercrime

Given the impact cybercriminals have on Canada and Canadians through ransomware and the theft of personal information, CSE has embarked on a long-term campaign designed to reduce the ability of cybercrime groups to target Canadians, Canadian businesses and institutions.

Working with Canadian and allied partners, CSE has helped reduce the ability of cybercriminals to launch ransomware attacks and to profit from the sale of stolen information.

Protecting democracy

CSE has the capabilities and the legal mandate to disrupt malicious online activity that threatens Canada's democratic processes. In the lead up to Canada's 2021 federal election, CSE had defensive cyber operations authorities in place to protect the electronic infrastructure used by Elections Canada. Had there been malicious cyber activity targeting the election process, CSE would have been ready to act on it right away.

> “We assess that ransomware will continue to pose a threat to the national security and economic prosperity of Canada and its allies in 2022 as it remains a profitable activity for cybercriminals.”
>
> **Canadian Centre for Cyber Security**
> *The Ransomware Threat in 2021*,[17]
> *December 2021*

Assisting the Canadian Armed Forces

CSE has also used its active cyber operations capabilities to assist the Canadian Armed Forces in support of their mission.

Communications security **(COMSEC)**

CSE is responsible for keeping the Government of Canada's sensitive communications secure.

For example, we supply devices that allow ministers and senior officials to communicate securely from anywhere. This function has become even more important during the pandemic. In February 2021 we partnered with the Privy Council Office and Shared Services Canada to add secure video to meet the ongoing need for virtual meetings at the classified level.

Demand for these services continued to grow this year. CSE continued to work with partners to support and expand functionality of these critical services. This included upgrading hardware and expanding access to the systems.

We also continued to operate Canada's Top Secret Network (CTSN). As the name suggests, this is a network used by Government of Canada departments, agencies and authorized contractors who need to store and share classified information up to the Top Secret level. This year CSE piloted CTSN Deployable Kits with a limited number of client departments. This makes it easier for departments to deploy CTSN connectivity in the field when a temporary installation is required.

Secure communications rely on strong cryptography to keep information secure and to protect systems from cyber threats.

Over the past year CSE has helped keep the Government of Canada's data secure by:

- supplying cryptographic tools, devices and expertise
- bringing in new cryptographic procedures
- advising government and industry on the use of cryptography and new cryptographic techniques, such as:
  - → quantum-resistant algorithms (see "Preparing for the post-quantum future")
  - → homomorphic encryption

We helped bolster assurance in the IT products Canadian organizations rely on by:

- certifying commercial IT products against international standards in:
  - → cryptography (Cryptographic Module Validation Program)[18]
  - → cyber security (Common criteria)[19]
- participating in international standards bodies

We also published guidance about encryption for Canadians and Canadian organizations:

- Using Encryption to Keep Your Sensitive Data Secure[20]

Cyber security: **federal institutions**

CSE's Cyber Centre is the operational lead for protecting the Government of Canada from cyber threats such as ransomware and cyber espionage. We work with federal partners, including Shared Services Canada and the Treasury Board Secretariat, to defend the networks and information of federal institutions. These include government departments, government agencies and Crown corporations. In this report, "departments" generally refers to departments and agencies.

Layered defences

The Cyber Centre uses autonomous sensors to detect malicious cyber activity on government networks, systems and cloud infrastructure. We use three types of sensors: network-based sensors, cloud-based sensors and host-based sensors[21] (on laptops, desktops and servers).

These sensors securely gather system data and feed it back to the Cyber Centre for analysis. Some critical infrastructure partners, including provinces and territories, also send us technical data from system security logs. This helps us protect them and improves our analytics for the Government of Canada and other partners. All of this happens with strict privacy controls in place.

Our automated tools and expert analysts search the data for unusual patterns. If we find malicious activity, we take action to thwart it. This includes directing our sensors to block it automatically.

Our automated defences protect the Government of Canada from between 3 and 5 billion malicious actions a day, ranging as high as 7 billion. These actions include:

- attempts to map systems and networks
- attempts to extract information from databases
- malicious domains (website names and email addresses)
- malicious IP addresses (the unique code identifying a computer or device on the Internet)

Every department within Shared Services Canada's Enterprise Internet Services (EIS) network perimeter benefits from this protection. This year, the Cyber Centre has also deployed host-based sensors in the context of providing cyber incident support to Canadian critical infrastructure.

As of March 2022:

- 70 federal institutions have deployed our cloud-based sensors
- 79 federal institutions have deployed host-based sensors on over 730,000 hosts

Protecting Crown corporations

Crown corporations are federal institutions and fall under CSE's cyber security mandate. However, they operate independently from the Government of Canada and are responsible for managing their own IT infrastructure. Each Crown corporation is free to choose their own level of support from the services available to critical infrastructure partners (see Cyber security services). Some Crown corporations are eligible for the full range of services available to core government departments.

In February 2022, the National Security and Intelligence Committee of Parliamentarians published a report on the Government of Canada's cyber defences. While recognizing Canada as a "world leader in defending its networks from cyber attack",[22] the Committee noted that many Crown corporations have not opted into the cyber defences offered by the Government of Canada, putting their data at increased risk. The report recommended that the government extend its advanced cyber defence services, including CSE's cyber defence sensors, to all federal organizations. The Government of Canada agreed with the recommendation and CSE is exploring options to implement it.

This is in addition to the cyber security services the Cyber Centre offers to critical infrastructure partners, including Crown corporations. In April 2021, the Cyber Centre established a dedicated point of contact for Crown corporations.

> For the Committee, the consequences of those choices are clear: not obtaining the government's cyber defence services means choosing to leave data and the integrity of systems vulnerable to the world's most sophisticated cyber threats.
>
> **National Security and Intelligence Committee of Parliamentarians**
> *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack*,[23] *February 2022*

Over the course of the year, we reached out to make sure every Crown corporation was aware of the full range of services available to them, and the potential benefits to their cyber security. As a result of this outreach, dozens more organizations signed up to receive Cyber Centre services. Several Crown corporations increased their level of service this year to match that of core government departments.

Incident management

It is the nature of cyber security that even with the best defences, cyber incidents do occur.

The Cyber Centre offers 24/7 support to contain the threat and mitigate the damage when cyber incidents affect federal institutions or systems of importance to the Government of Canada.

This fiscal year, the Cyber Centre opened 2,023 cyber security incident cases. That's an average of 5.5 per day. Of those cases, 1,154 were federal institutions, and 869 were critical infrastructure.

The types of incidents included:

- reconnaissance activity by sophisticated threat actors
- phishing incidents (emails containing malware)
- unauthorized access to corporate IT environments
- imminent ransomware attacks
- zero-day exploits (exploitation of critical vulnerabilities in unpatched software)

Depending on the nature and severity of the case, the incident management team offers:

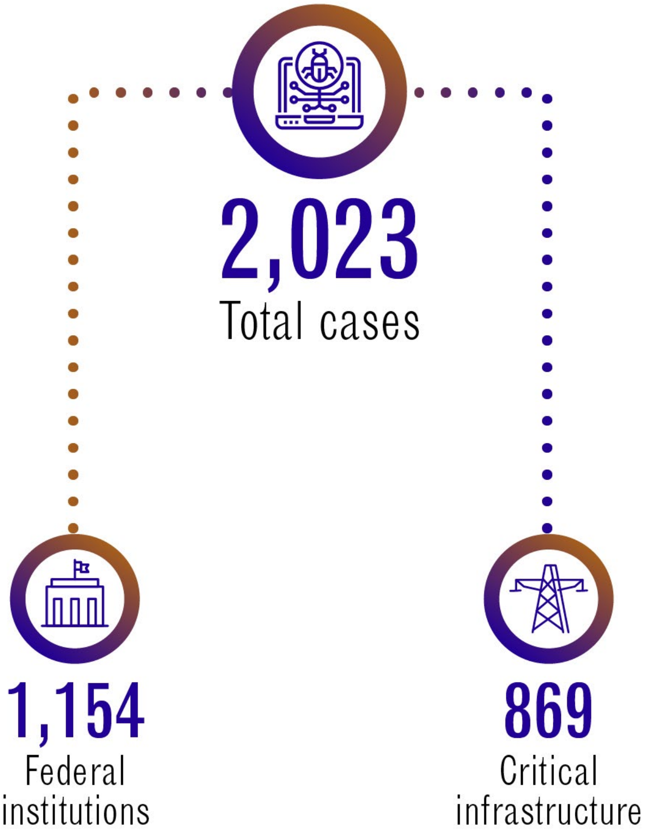
- victim notifications
- tailored advice and guidance
- recovery assistance
- analysis reports
- digital forensics

We offer these services day in day out. This year, the Cyber Centre also provided incident response coordination and standby support for major planned events including:

- the 2021 Canadian federal election
- the 2021 Canadian census
- the COVID-19 vaccine rollout

> **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*[24]

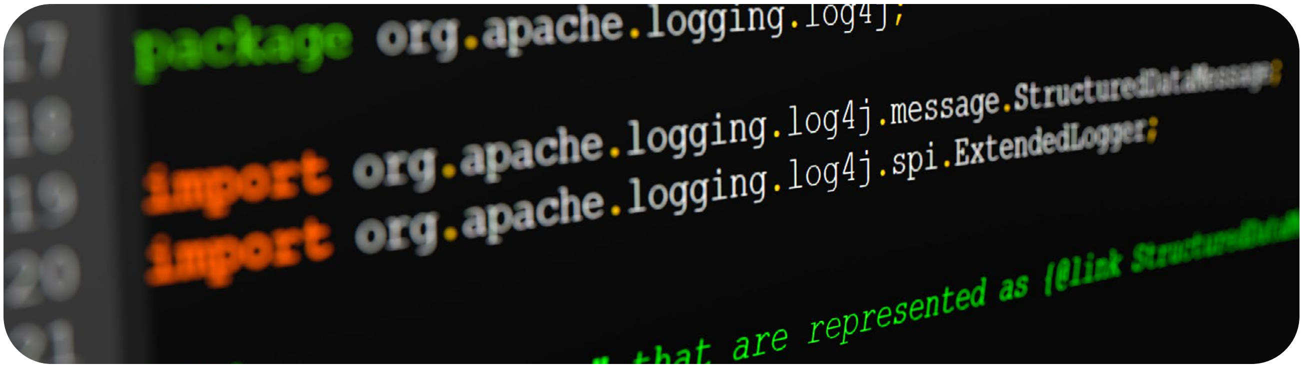
Cyber security incident cases 2021 to 2022



2,023
Total cases

1,154
Federal institutions

869
Critical infrastructure



```
package org.apache.logging.log4j;

import org.apache.logging.log4j.message.StructuredDataMessage;
import org.apache.logging.log4j.spi.ExtendedLogger;

 * that are represented as {@link StructuredData
```

Case study: the Apache Log4j vulnerability

In December 2021, organizations around the world were affected by a zero-day vulnerability in a widely used software product: Apache Log4j.

The vulnerability meant threat actors could access affected devices remotely to steal information, including passwords and logins, or to infect networks with malicious code.

Cyber Centre teams acted quickly to notify government partners and Canadian organizations. In total we published 8 alerts.

The Cyber Centre coordinated the federal response to make sure other government departments and critical infrastructure providers were aware of the threat and knew how to mitigate it.

Data from our host-based sensors helped us to identify affected devices quickly to assist departmental IT teams in their remediation efforts.

Cyber Centre analysts identified domains and IP addresses associated with the vulnerability and blocked them at the network perimeter.

This cyber vulnerability could have had severe consequences. Thanks to our automated defences, skilled specialists, and strong collaboration with IT teams from Shared Services Canada, Treasury Board Secretariat and many other Government of Canada departments, it was contained and neutralized before it could cause significant damage.

Working with partners

The Cyber Centre does not act in isolation. We coordinate with federal, international and industry partners.

As Canada's national Computer Security Incident Response Team (CSIRT), the Cyber Centre works with other national CSIRTs around the globe to exchange information and expertise. This helps each country's CSIRT notify victims and resolve incidents more quickly.

In the fall of 2021, the Cyber Centre and our federal partners formalized an operational group to better coordinate the response to cyber incidents with potential national security implications. The National Cyber Response Unit comprises units from:

- CSE
- The Canadian Armed Forces (CAF)
- Canadian Security Intelligence Service (CSIS)
- RCMP
  - → The National Cybercrime Coordination Unit (NC3)
  - → Federal Policing

Removing spoofs

Cyber criminals create fraudulent websites, email domains and social media profiles to try to trick Canadians into sharing personal information or clicking on infected links.

When these spoofs mimic government departments or officials, it undermines trust in the real sources, and it puts Canadians at risk of getting scammed.

From the start of the pandemic to March 31, 2022, the Cyber Centre worked with trusted industry partners and international allies to take down over 11,500 of these fake domains.

Cyber security: **critical infrastructure**

CSE has a mandate to help improve the cyber resilience of Canada's critical infrastructure (CI). This is a top priority for the Cyber Centre, and much of our focus this year has been about deepening and expanding our CI partnerships.

CI means the essential services we can't do without, like healthcare, energy, finance, and communications. It is a lucrative target for ransomware gangs.

CI also faces threats from state-sponsored cyber actors, who may target CI assets as a form of geopolitical leverage. In early 2022, the Cyber Centre issued two threat bulletins[25] alerting critical infrastructure about known Russian-backed cyber threat activity.

If CSE learns of a cyber threat, either through foreign signals intelligence, or while maintaining the government's cyber defences, we share that information with as many trusted critical infrastructure providers as possible.

> **In 2021, the Cyber Centre was aware of 304 ransomware incidents against Canadian victims, over half of them in critical infrastructure. But we know cyber incidents are significantly underreported, and the true number of victims is much higher.**
>
> **Sami Khoury**
> *Head of the Canadian Centre for Cyber Security*

Case study: support to Newfoundland and Labrador

In the fall of 2021, the healthcare system of Newfoundland and Labrador was impacted by a serious cyber incident. Thousands of medical procedures had to be cancelled and thousands of patient files were breached.[26]

The Cyber Centre worked closely with the province and our federal partners to coordinate the IT portion of the response. This included sending a team to provide hands-on cyber security support. Over the course of several months the Cyber Centre provided:

- on-site support (3 weeks)
- remote assistance
- tailored advice and guidance
- digital forensics
- mitigation (recovery) assistance
- information sharing
- analytical reports
- advice on rebuilding infrastructure

New funding in Budget 2022 will enable the Cyber Centre to offer more help of this kind in the event of high-impact cyber incidents on Canada's critical infrastructure.

Key sectors

This year the Cyber Centre has engaged approximately 1000 critical infrastructure partners across a range of sectors including:

- academia
- Crown corporations
- democratic institutions
- energy
- finance
- health
- information and communications technology
- provinces / territories / municipalities*
- small and medium organizations
- transport

*Note: "municipalities" includes some city-run services including police and fire services and water utilities.

Cyber security services

The Cyber Centre encourages eligible CI partners to sign up for our free, confidential cyber security services. These include, but are not limited to:

- incident management
- threat intelligence
  - → alerts about cyber threats (plus mitigation steps)
  - → weekly incident summaries
  - → regular cyber threat briefings
  - → notifications about malicious activity on their IP space
- access to our malware analysis platform
- access to our automated threat intelligence feed
- sector-specific community outreach and engagement
- a dedicated Cyber Centre point of contact

Our services do not replace commercial solutions, but they help CI providers tailor their cyber defences based on reliable information and expert advice. Partners can choose the level of service that best meets their needs, or engage with the Cyber Centre for advice and guidance as and when they need it.

Malware analysis platform

Assemblyline[27] is the Cyber Centre's malware detection and analysis platform. Analysts submit suspicious files, and Assemblyline checks them against the Cyber Centre's unique database of cyber threats. If the sample is malicious, Assemblyline provides details about the malware strain to help inform the response.

At first, Assemblyline could only be used within CSE on our classified network, where we use it to help defend the Government of Canada from cyber threats. But over the years, we have found ways to share it externally, so that other cyber defenders can benefit from it.

CSE first released the software for Assemblyline in 2017, allowing others to build their own platforms using our code. Over 3,000 organizations downloaded these do-it-yourself versions of Assemblyline. Since then, the Cyber Centre has re-written Assemblyline from the ground up.

The latest version, Assemblyline 4,[28] is cloud-compatible, and it has a new database, a new user interface and new malware detection capabilities. We released it open source in January 2020 and completed its implementation on our classified network in February 2022.

In the interim, we created two new Assemblyline platforms that our external partners can use for free: one for government clients and one for critical infrastructure partners. This was made possible by major investments in our IT infrastructure during the pandemic. With that groundwork done, we can support more services at the unclassified level and Protected B (a mid-level security classification)[29].

Now, instead of emailing samples to the Cyber Centre and waiting days for a manual analysis, external partners simply log in, submit their suspicious files for analysis and get a result within minutes.

Summary of Assemblyline 4 releases

Date	Format	Audience	Classification	Number of organizations
January 2020	Open-source software	Anyone	Unclassified	Not tracked
July 2020	External-facing platform	Government clients	Protected B	32 departments
March 2021	External-facing platform	Critical infrastructure	Unclassified	133 organizations
February 2022	Upgrade to internal platform	CSE cyber defenders	Classified	No external clients

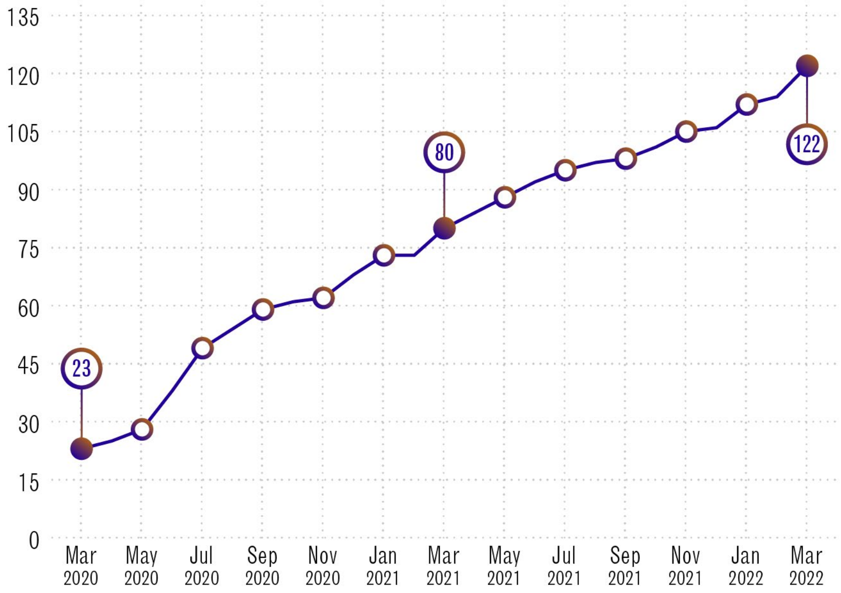
Automated threat intelligence feed

Aventail is the Cyber Centre’s automated threat intelligence sharing service. It provides critical infrastructure partners with relevant, verified information about Indicators of Compromise (IoCs) at machine speed. IoCs are details about cyber threats, such as:

- domains and URLs (elements of web addresses)
- IP addresses (numeric codes that identify devices on the Internet)

Cyber defenders use IoCs to prevent and mitigate malicious activity on their networks. This year, Aventail shared 46,965 unique IoCs. That’s an average of 129 a day.

AVENTAIL partners



CSE has shared its threat feed with Government of Canada departments and our Five Eyes partners since 2017. In March 2020, the Cyber Centre launched Aventail so we could share it directly with CI partners. This year our client base for Aventail has grown from 80 to 122 CI partners.

The Cyber Centre also shares Aventail with CIRA (the Canadian Internet Registration Authority) to enhance their threat-blocking service, Canadian Shield.

Aventail is part of the Cyber Centre’s strategy to create tools and build partnerships that raise the bar for cyber security in Canada.

Protecting Canada's energy infrastructure

In February 2021, the Prime Minister of Canada and the President of the United States announced a Roadmap for a Renewed US-Canada Partnership,[30] which included a commitment to enhance the cyber resilience of our shared cross-border energy infrastructure. This year, the Cyber Centre continued to work with Canadian and US partners in support of this shared strategic priority.

For example, in August 2021, Natural Resources Canada (NRCan) announced federal funding for the Blue Flame Program.[31] The initiative is a two-way information sharing partnership between the Cyber Centre and the Canadian Gas Association (CGA).

Participating organizations have the option to share their network data with the Cyber Centre for analysis, which gives the Cyber Centre a more accurate picture of the threats affecting the natural gas sector. In return, the Cyber Centre is able to share a tailored threat feed with CGA members.

The partnership with the CGA follows a model established between the Cyber Centre and Ontario's Independent Electricity System Operator (IESO) under IESO's Lighthouse[32] initiative. Both collaborations are ongoing in 2022.

> **(The) likelihood of a cyber attack impacting the Canadian electricity sector is higher than it otherwise might be because of the connections between US and Canadian grids.**
>
> **Canadian Centre for Cyber Security**
> *The Cyber Threat to Canada's Electricity Sector,*[33]
> *November 2020*

Protecting the health sector

As mentioned in last year's CSE Annual Report,[34] cyber threats against Canada's health sector increased during the pandemic, prompting the Cyber Centre to sign up over 100 new health organizations in 2020 to 2021 to receive cyber security services. Engagement remained strong this year with roughly 140 organizations regularly attending virtual briefings for the health community.

In March 2021, the Cyber Centre began an urgent program to boost the cyber security of the COVID-19 vaccine rollout and pandemic response. The program, Canadian Armour, was open to Canadian organizations involved in the development or delivery of COVID-19 vaccines.

The Cyber Centre contracted CIRA to provide licensing for their DNS Firewall service. DNS stands for Domain Name System and acts like a directory for the Internet, converting human-readable web addresses into machine-readable IP addresses. A DNS firewall protects users by blocking their connection to known malicious websites.

In addition to the DNS Firewall protection, health organizations also benefitted from Cyber Centre analysis. We analyzed the DNS traffic and found potentially malicious domains that were previously unknown. We reported these to the organizations to investigate and mitigate possible compromises.

Nine organizations took part in the program, including hospitals, health authorities and bio-pharmaceutical manufacturers. The licensing portion of the program wrapped up at the end of March 2022, but the Cyber Centre analysis continues for participating organizations.

Protecting democratic institutions

The 2021 Canadian federal election was held on September 20, 2021. Drawing on CSE's experience in past elections, the Cyber Centre worked in partnership with Elections Canada to:

- ensure strong and effective cyber defence measures were in place to protect Elections Canada's systems and networks
- prepare and conduct a cyber themed Table-Top Exercise (TTX) to test decision-making and coordination processes
- provide cyber incident management and monitoring during the election period

The Cyber Centre reached out to all registered federal political parties to determine their top-of-mind cyber security concerns. Based on that feedback, we offered guidance and threat briefings to meet those priorities.

We worked with the Leadership Debates Commission and the Canadian Museum of History (the venue for the Leadership Debates) to review their IT infrastructure and provide cyber security advice.

Outside of federal election periods we continued to work with the Privy Council Office to support Canada's democratic institutions including:

- Elections Canada
- registered federal political parties
- provincial and territorial elections authorities

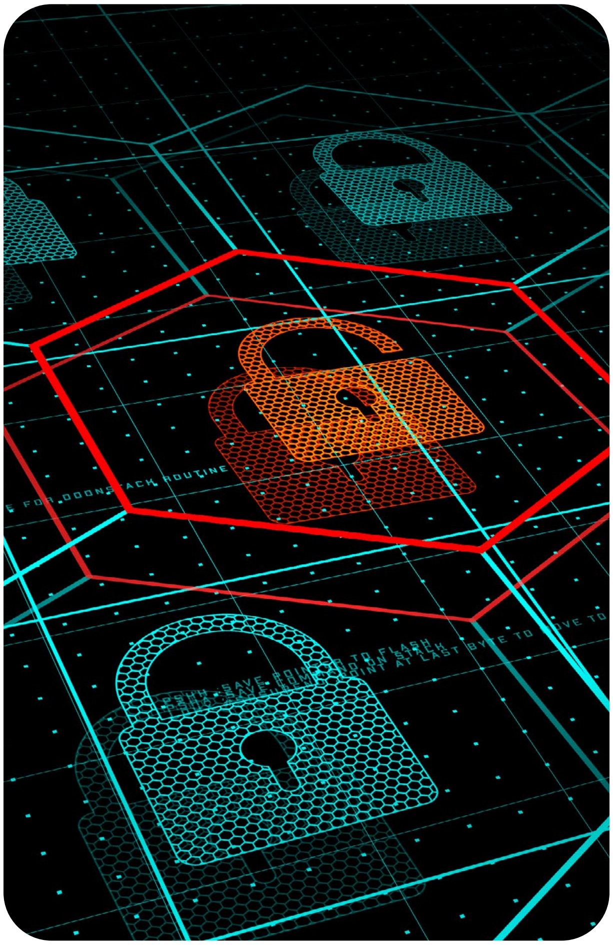
We produced guidance on topics of concern to this sector including guidance publications and a new Learning Hub training course on cyber security for political parties.[35]

Protecting Canadians from phishing

Phishing attempts are sadly all too familiar. They are unsolicited messages from cyber criminals trying to scam people. They may be phone calls, emails, social media direct messages or SMS texts (smishing).

The Cyber Centre is working with select partners in the telecommunications and finance sectors to protect Canadians from phishing and smishing. Partners share suspected malicious websites with each other. Each partner can vet and use the information according to their own mandate. For instance, the Cyber Centre can add the website to its block list or notify trusted industry partners to take the site down.

In September 2021, the Cyber Centre launched a new sharing hub to vet and document these cyber threats automatically. As a result, partners can now mitigate these cyber threats at machine speed to better protect Canadians against phishing.



Surveying small and medium organizations

In the fall of 2021, the Cyber Centre and the BC Chambers of Commerce conducted a survey of Canadian small and medium-sized organizations about their cyber security.[36] The results showed that:

- the majority of businesses (61%) had experienced a cyber security incident
- only a quarter of those victims (26%) had reported the incident to law enforcement
- most business owners (85%) were not aware that the Government of Canada offers cyber security supports to small and medium organizations
- more than half (52%) of business owners did not know where to report a cyber crime

In response to the survey, the Cyber Centre worked with federal partners to develop an awareness publication about the available cyber security resources for small and medium organizations.[37] The Cyber Centre is also designing a basic "Essential 5" toolkit for business that contains the minimum cyber security controls in a user-friendly checklist format.

New cyber incident reporting portal

In May 2021, the Cyber Centre launched a new feature on our website, to make it easier to report a cyber incident.[38]

Cyber incident reporting helps the Cyber Centre keep Canada and Canadians safe online by giving us a more accurate picture of the cyber security landscape. We use that information to inform our advice, guidance and services.

The portal allows government departments, critical infrastructure providers and IT practitioners to report incidents directly to the Cyber Centre. Depending on the circumstances we can offer them advice and guidance.

The portal directs Canadian individuals and small or medium organizations to the right partner for different incident types. For instance, the RCMP or local police handle cybercrime investigations, while the Spam Reporting Centre gathers complaints about unsolicited emails and texts.

Building Canada's **digital resilience**

CSE improves Canada's overall digital resilience by sharing information, advice and training.

Sharing our threat feed to benefit Canadians

The Cyber Centre works with trusted partners to improve cyber security for Canadians in their daily lives. Our partnership with CIRA is a prime example.

CIRA Canadian Shield[39] is a free service that protects Canadians' privacy on their home networks and personal devices. It also has a threat-blocking option that prevents users from inadvertently connecting to known malicious sites. The Cyber Centre shares its automated threat intelligence feed with CIRA, so that any threats we have identified will also be blocked by Canadian Shield.

As of March 31, 2022, more than 177,000 users have signed up for Canadian Shield's threat-blocking services, which recorded more than 88 million blocks this year.

Reports and guidance

The Cyber Centre raises awareness and builds cyber resilience through public reports and guidance.

Reports and assessments

This year the Cyber Centre published 3 in-depth reports:

- Cyber Threats to Canada's Democratic Process: July 2021 Update[40]
- The Cyber Threat to Operational Technology[41]
- The Ransomware Threat in 2021[42]

We also published 2 short bulletins on Russian-backed cyber threat activity.[43] Our cyber threat reports are based on a combination of classified and public sources, including:

- open-source industry reporting
- operational knowledge from CSE's cyber defence operations
- classified intelligence from CSE's foreign signals intelligence program
- intelligence from our Five Eyes partners (US, UK, Australia and New Zealand)

Guidance publications

The Cyber Centre published 30 advice and guidance publications[44] this year. We added a filtering capability to our website to make it easier for Canadians to find the resources they are looking for.

Due to the surge in ransomware incidents over the last couple of years, in December 2021, the Cyber Centre created a dedicated ransomware page[45] on our website. The page includes threat reports, guidance resources and an open letter to Canadian organizations signed by four Canadian government ministers. The new Ransomware Playbook[46] contains detailed advice on how to defend against ransomware, as well as how to recover in the event of an incident.

Our guidance publications this year addressed some of the most common "weak links" exploited by ransomware attackers, including:

- Digital footprint[47]
- Security considerations for your website[48]
- Spotting malicious email messages[49]
- Strategies for protecting web application systems against credential-stuffing attacks[50]

Several guidance publications focused on threats to critical infrastructure:

- Security considerations for industrial control systems[51]
- Protect your medical research equipment from cyber threats[52]
- Cyber security considerations for connected medical devices[53]

We also developed guidance on priority topics for democratic institutions, including:

- How to identify misinformation, disinformation and malinformation[54]
- Securing access controls in a volunteer-based organization[55]
- Security considerations for electronic poll book systems[56]
- Security considerations when using social media in your organization[57]

Alerts and advisories

The Cyber Centre issues alerts and advisories for IT professionals. These outline recommended actions on specific cyber threats ranging from routine software updates (advisories) to critical vulnerabilities (alerts).

For example, in December 2021, the Cyber Centre published 1 joint advisory[58] and 8 alerts[59] about the Apache Log4j vulnerability.

These alerts and advisories are posted on our website and social media channels. We also email alerts directly to Cyber Centre clients. As of March 31, 2022, 2701 contacts from 832 organizations subscribed to this service.

Cyber Centre public reports by the numbers

679 Advisories

46 Alerts

30 Advice and guidance publications

5 Cyber threat reports

Get Cyber Safe

Get Cyber Safe (GCS) is a national public awareness campaign that provides simple cyber security advice Canadians can apply in their everyday lives. In November 2021, Get Cyber Safe marked 10 years[60] of helping Canadians stay safe online.

GCS resources

Ransomware was a priority theme for Get Cyber Safe this year:

- Be prepared: how your business can protect itself from ransomware attacks[61]
- Ransomware 101: How to stay cyber secure[62]
- Video: Malware and ransomware[63]
- Ransomware: Back up your data, or else![64]

GCS produced several new resources for older Canadians this year, including:

- Cyber security checklist[65]
- How older adults can protect themselves from the most common cyber security threats[66]
- Real examples of fake emails[67]
- Get cyber safe to protect your time online[68]

At the other end of the age spectrum, GCS shared content for youth and families, such as:

- Cyber threats families need to watch out for[69]
- What's in your cyber security backpack[70]
- How to avoid sharing too much information online[71]
- A workbook[72] with games and quizzes about "Cyber Agent training"

In December 2021, Get Cyber Safe spread seasonal joy and cyber security awareness with:

- the Get Cyber Safe Gift Guide 2021[73]
- a Festive Yule Firewall video[74]
- downloadable Gingerbread Home Network Kits[75]

The firewall video features cyber security-themed holiday carols in both official languages. The gingerbread kits include tips for securing your home router and laptop in between decorating steps. CSE sent physical gingerbread kits to 27 external partners, 18 of whom helped to amplify our advice by sharing their creations on social media.

Cyber Security Awareness Month

October is Cyber Security Awareness Month[76] (CSAM) in Canada. This year’s theme was “Life Happens Online” reflecting how the Internet has kept us connected during the pandemic. Get Cyber Safe is the lead organizer of CSAM in Canada. We work with external partners to boost cyber security awareness through:

- shareable resources[77]
- speaking engagements

This year, we grew our CSAM partner list to over 300 organizations (up 35%) and received double the number of speaker requests. We co-created content with:

- the Canadian Bankers Association
- CIRA
- MediaSmarts
- Microsoft

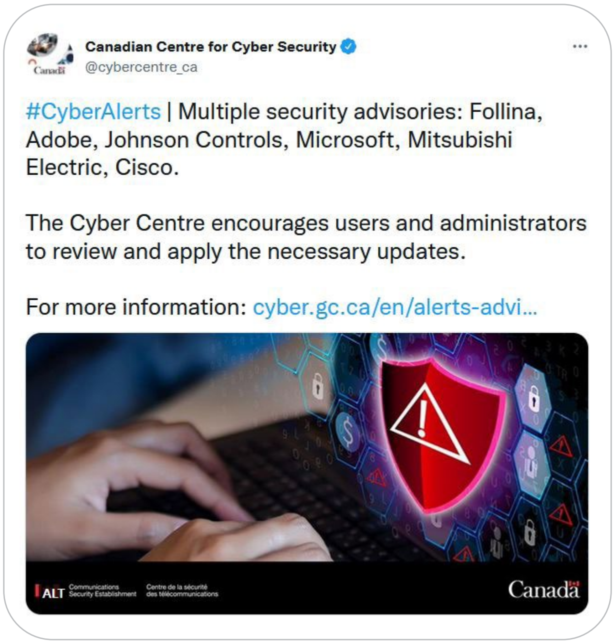
At least 247 partners shared CSAM content, including:

- federal institutions
- provinces, territories and municipalities
- industry partners

Social media

Our social media team publishes content daily from CSE, the Cyber Centre and Get Cyber Safe. This year, our social media feeds shared information about:

- cyber security alerts and advisories
- cyber security tips and resources
- public reports
- job opportunities and recruitment events
- CSE’s mandate and history
- equity, diversity and inclusion initiatives at CSE
- outreach initiatives
- work with international partners


Canadian Centre for Cyber Security
@cybercentre_ca

#CyberAlerts | Multiple security advisories: Follina, Adobe, Johnson Controls, Microsoft, Mitsubishi Electric, Cisco.

The Cyber Centre encourages users and administrators to review and apply the necessary updates.

For more information: cyber.gc.ca/en/alerts-advi...

ALT
Communications Security Establishment
Centre de la sécurité des télécommunications
Canada

Social media by the numbers

CSE's social media presence is made up of 17 accounts across five platforms: Twitter, Facebook, LinkedIn, Instagram and YouTube. These accounts represent CSE, the Cyber Centre and Get Cyber Safe in both official languages. Combined, CSE's posts published from April 1, 2021, to March 31, 2022, were seen 6.6 million times.

With around 55,000 followers overall, Get Cyber Safe (GCS) has our largest presence on Twitter: more than CSE and the Cyber Centre combined. The number of people following GCS on Twitter held steady this year and dipped very slightly on Facebook. All our other accounts increased their overall followers by between 13% and 43%.

The following table shows the combined English and French followers of our social media accounts as of March 31, 2022. Numbers are rounded to the nearest thousand. The percentage change is year-over-year.

Platform	Account	Followers	Change
🐦	CSE	21,000	13%
	Cyber Centre	27,000	38%
	Get Cyber Safe	55,000	0.4%
f	Get Cyber Safe	52,000	- 1.4%
in	CSE	10,000	43%
	Get Cyber Safe	2,000	38%
📷	CSE	2,000	-
	Get Cyber Safe	3,000	28%
▶	CSE	500	43%

The Learning Hub

The Learning Hub is based at the Cyber Centre and provides training to improve the cyber security of Canada's government and critical infrastructure organizations.

The Learning Hub in 2021 to 2022

3,783 Participants

70 Private group training sessions

120 Public course offerings

13 Updated courses

3 New eLearning courses (13 total)

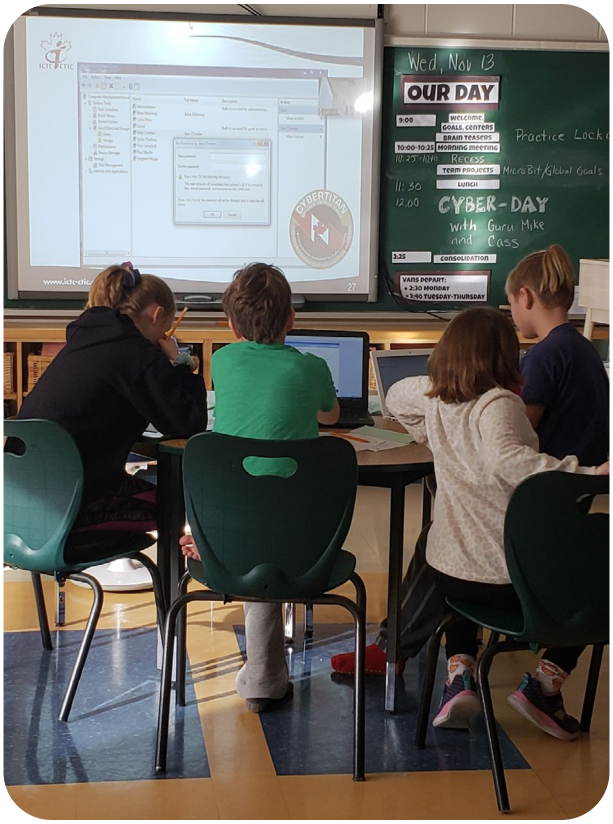
4 New cyber security courses (23 total)

Training for small and medium organizations

The Learning Hub worked with Innovation, Science and Economic Development Canada (ISED) to develop free cyber security training for small and medium organizations. ISED's CyberSecure Canada eLearning series[78] consists of 14 self-paced modules for learners with minimal technical knowledge. The modules can be taken as part of ISED's CyberSecure certification process, or simply to improve cyber awareness and resilience.

Training for public servants

This year, the Learning Hub renewed their collaboration with the Canada School of Public Service (CSPS) to provide a standardized cyber security curriculum for all federal public servants. For example, the Learning Hub and CSPS co-developed an e-learning course to introduce public servants from non-technical backgrounds to the basics of cloud computing. This is a priority topic for the public service as departments continue to migrate their IT infrastructure to the cloud.



Academic outreach

Canada needs a workforce with cyber skills, and that need is only going to grow. The Cyber Centre is working with academic institutions to build Canada's pool of cyber security talent. This year the Academic Outreach and Engagement team:

- advised academic institutions on curriculum content
- maintained up-to-date resources about careers in cyber security, including:
  - → certifications[79]
  - → post-secondary programs[80]

Community engagement

CSE runs community engagement[81] activities to raise cyber security awareness and inspire the next generation of cyber defenders.

While pandemic measures continued to limit our in-person activities in 2021, CSE volunteers gave six virtual presentations to around 200 school students across Ontario, on how to keep their devices and accounts safe. CSE volunteers also ran several virtual Raspberry Pi sessions for francophone schools in the National Capital Region.

CSE renewed our partnership with Hackergal, a Canadian non-profit that teaches girls, trans girls and non-binary students to code. We provided content for Hackergal's social media campaigns including for Privacy Awareness Day and Black History Month. CSE volunteers also:

- mentored students
- judged hackathon submissions
- sat on virtual panels
- gave speeches
- wrote blogs
- created learning videos

We also continued our partnership with CyberTitan, providing content and a keynote speaker for their online cyber defence competition for Canadian youth in grades 7 to 12.

> **With CSE's support, Hackergal has brought coding and digital literacy skills to over 25,000 girls and girl-identified learners across Canada since 2017. We're proud to partner with CSE to break down barriers for girls and help close Canada's gender gap in tech.**
>
> **Lucy Ho**
> *Executive Director at Hackergal*

Innovation

Technology is constantly evolving. CSE devotes time, energy and expertise to find new solutions to the challenges we face today and the ones we expect to face in the future.

Academic research

The Tutte Institute for Mathematics and Computing[82] (TIMC) is a research institute based at CSE. Its researchers work with colleagues in academia and industry to tackle scientific challenges related to CSE's mission.

Over the past year, TIMC researchers have worked with partners inside and outside CSE on research problems, including:

- detecting fake social media profiles using machine learning
- reducing the number of false positives in malware detection
- processing encrypted data without first decrypting it
- speeding up the detection of spam and phishing emails by grouping similar traffic into clusters
- using artificial intelligence to separate malicious network activity from activity that is unusual but benign

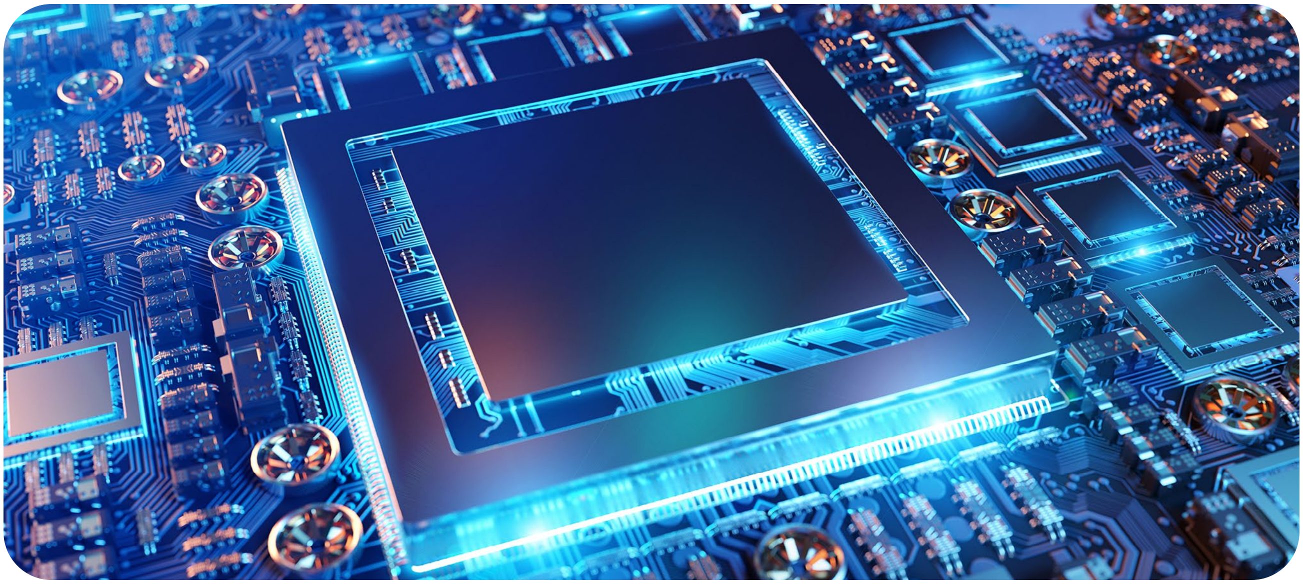
TIMC also conducted research related to cryptography and post-quantum cryptography (see next section).

While some aspects of TIMC's work are classified, whenever possible the institute releases its original research to benefit the external open-source and research communities. Over the past year, TIMC researchers have published:

- articles in peer-reviewed journals
- conferences papers
- open-source code releases
- a textbook

TIMC researchers organized 7 virtual conferences and participated in dozens of others. Software libraries from TIMC are averaging over 2.5 million downloads per month.

In December 2021, TIMC marked its tenth anniversary.



Preparing for the post-quantum future

From online banking to emails and instant messages, we use cryptography every day to store and send data securely. But experts predict that, as early as the 2030s, quantum computers[83] could be powerful enough to break the cryptography used today.

That's why CSE is working to prepare Canada for the post-quantum future.

CSE is working with partners in industry, academia and the National Research Council of Canada to better predict when quantum computers might reach the breakthrough point. This informs the Cyber Centre's guidance on the risk to government and critical infrastructure.

Cryptography uses specialized techniques (encryption and authentication) to keep information confidential and to protect systems from cyber threats. The Cyber Centre and CSE's Tutte Institute for Mathematics and Computing are studying new cryptographic techniques and the mathematics they are based on to find quantum-resistant solutions.

The National Institute of Standards and Technology (NIST) in the United States has led a four-year international selection process to standardize quantum-resistant cryptography for widespread use. The Cyber Centre has analyzed these technologies to make sure Canadians can rely on them to protect their information well into the future.

Later this year, NIST is expected to announce the selection of the first general-purpose quantum-resistant cryptography to be standardized. This will be a major step in the journey towards reliable post-quantum applications.

Collaborative problem-solving

CSE hosts various collaborative events to drive cyber security innovation.

BigDig

BigDig is a 2-week classified event hosted annually by the Cyber Centre to tackle high-priority cyber security challenges. Participants come from across the Government of Canada, our Five Eyes partners, and select Canadian industry partners. They must have a valid security clearance to use CSE's classified resources.

In November and December 2021, BigDig participants made advances in areas including:

- incident detection
- malware analysis
- defensive cyber operations capabilities
- securing the Internet of Things (IoT)

GeekWeek

GeekWeek is the Cyber Centre's annual cyber security workshop at the unclassified level. It brings together participants from government, industry and academia. Every year GeekWeek participants work on more than 30 different projects to solve hard cyber security problems.

Past GeekWeek events have taken place in the fall, but future events will be held in the spring. As a result of that switch, there was no GeekWeek this year. However, the work begun at GeekWeek events continues year-round as CSE employees find ways to take ideas from proof-of-concept to implementation.

For example, Chameleon is a configurable software that can be used offline as a network simulator, or online as a network honeypot. A honeypot is a decoy target used to attract cyber threat activity in order to study it and defend against it. Chameleon was developed over the course of 4 GeekWeek events by over 50 participants from different organizations. It can currently emulate more than 154 cyber security vulnerabilities.

In March 2022, the Cyber Centre finalized the code for Chameleon and released it back to the GeekWeek community for a Canadian wide impact.

GeekWeek innovations have contributed to many other Cyber Centre tools including several mentioned in this report:

- Assemblyline
- Aventail
- Tracker
- the sharing hub to help protect Canadians against phishing

GeekPeek

New this year, GeekPeek is an unclassified hackathon for Canadian graduate and undergraduate students in fields related to cyber security.

In December 2021, the Cyber Centre welcomed 26 students from 7 universities across Canada for the first edition of GeekPeek. For 5 days, they worked with Cyber Centre professionals on problems related to:

- machine learning
- network traffic analysis
- cyber threat hunting
- malware reversing

From January to March 2022 the Cyber Centre ran a "capstone edition" of GeekPeek in collaboration with Queen's University. Cyber Centre employees mentored 25 students working on their capstone projects (applied research in the final year of study). Cyber Centre judges evaluated the projects at the end of March, with the best presentations shown at GeekWeek 2022.

Developing and improving cyber security tools

The Cyber Centre designs and shares tools so that government departments can assess their own cyber security more efficiently. Below are some examples of technologies we improved upon this year.

Observation Deck

Observation Deck is a web application the Cyber Centre offers to government departments in our host-based sensor program. The platform lets users view data from the sensors on their department's IT infrastructure so they can make informed decisions about their cyber security.

More than 40 departments have adopted Observation Deck since its launch in 2020. In November 2021, the Cyber Centre rolled out a new version based on user feedback. The redesign has better search functionality and new reporting views. It also lets users generate and export datasets, including custom charts.

Over the past year, the Cyber Centre has used Observation Deck to help our partners respond to numerous cyber security events, including Log4j and #PrintNightmare.

ASTRA (Analytical Software for Threat Assessment)

ASTRA is a threat risk assessment tool created by the Cyber Centre to help Government of Canada departments evaluate the level of cyber risk to their IT assets. For example, it could be used at the beginning of a project to evaluate the cyber security of different network architectures.

The interface walks users step by step through the risk assessment process, similar to the way income tax software helps you fill in a tax return.

ASTRA allows users to:

- identify risks of concern
- recommend solutions
- track risk levels over the course of a project

Prior to this year, ASTRA existed as a standalone platform hosted by the Cyber Centre. In March 2022, the Cyber Centre released an enterprise version of ASTRA which client departments could download onto their own networks. This allows whole teams to work with the same information and makes the whole process more convenient. By the end of the fiscal year, 53 departments had downloaded ASTRA to help them assess their cyber risks.

Tracker

Tracker is an automated self-assessment tool for Government of Canada departments and agencies. The interactive platform allows users to check the security configuration of their public facing websites and email services. This helps to:

- prevent cyber criminals from spoofing government email domains
- secure the online services Canadians rely on
- protect the reputation of the Government of Canada

Tracker was co-developed by the Cyber Centre and the Treasury Board of Canada Secretariat (TBS) based on TBS's HTTPS-Everywhere[84] tool. The updated version makes it easier for departments to check their compliance with both TBS policy and Cyber Centre guidance. It launched in October 2021 and is being used by close to 100 Government of Canada organizations.

Accountability

CSE strives to be as transparent as possible, so that Canadians can be confident that we respect the law and protect their privacy.

Transparency

As part of the National Security Transparency Commitment,[85] CSE works to help our clients, partners, review agencies, and all Canadians understand who we are and what we do, while ensuring that privacy and security are protected.

This fiscal year, CSE released information about our activities through:

- public reports[86]
- parliamentary appearances
- proactive disclosures[87]
- Access to Information requests[88]
- Open Government releases[89]

This is in addition to our external communications, including:

- news releases
- media interviews
- social media content
- public speeches
- web content

Internal compliance

The *CSE Act* dictates what CSE can and cannot do under the law. How we put those authorities into practice is detailed in our Mission Policy Suite.

This set of operational policies was developed in consultation with the Department of Justice, and is based on Canada's laws and values, as well as decades of both internal and external reviews.

CSE works to make sure employees know their legal and policy obligations under the Mission Policy Suite. We foster a culture of compliance by:

- encouraging employees to self-report any possible compliance incidents
- working with employees to address concerns and incidents
- performing our own internal verification activities
- building compliance requirements into training, systems, tools and processes

This year, CSE's internal compliance team conducted:

- annual compliance training
- knowledge testing
- routine monitoring
- engagement initiatives

External oversight

The Minister of National Defence guides and authorizes CSE activities using a combination of Ministerial Directives, Authorizations, and Orders, which establish operating parameters and expectations for CSE.

As an added layer of accountability, the Intelligence Commissioner (IC) provides independent external oversight of CSE's Foreign Intelligence and Cyber Security Authorizations. The Minister must issue an Authorization for any activities that would otherwise:

- contravene an Act of Parliament
- interfere with the reasonable expectation of privacy of a Canadian or anyone in Canada

For example, an Authorization is required for CSE to provide cyber security services to another federal government department that could potentially impact a Canadian's reasonable expectation of privacy. The Minister can only issue an Authorization if they conclude that the conditions of the *CSE Act* are met, including that the activities are reasonable and proportionate, and that there are measures in place to protect the privacy of Canadians and persons in Canada.

CSE then provides the IC with all the information, written or verbal, that was given to the Minister. The IC must then decide whether the Minister's conclusions are reasonable. CSE cannot carry out the activities until the IC approves the Authorization.

CSE submitted a total of 5 Ministerial Authorizations to the IC in 2021:

- 3 Foreign Intelligence Authorizations
- 2 Cyber Security Authorizations

The IC fully approved 4 of the 5 Authorizations.

The IC partially approved 1 Foreign Intelligence Authorization, requiring CSE to provide more information about a specific activity proposed within it. CSE will submit more detailed information on this activity in a future application. Until then, CSE continues to conduct only the activities approved by the IC.

Ministerial Authorizations submitted by CSE to the Intelligence Commissioner in 2021[90]

Authorization type	Submitted	Approved	Not approved	Partially approved
Foreign Intelligence	3	2	-	1
Cyber Security	2	2	-	-
Amendments to authorizations	-	-	-	-
Total	**5**	**4**	**-**	**1**

External review

As with any other federal department or agency, CSE's activities are subject to review by various federal bodies, including the Privacy Commissioner, Information Commissioner, Auditor General, Canadian Human Rights Commission, and Commissioner of Official Languages.

In addition, CSE is subject to review by two independent external review bodies with a national security and intelligence mandate:

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

NSIRA is responsible for reviewing national security and intelligence activities across the Government of Canada. NSICOP consists of members from both Houses of Parliament from all major parties with a broad mandate to review Canada's national security and intelligence organizations.

Together, these external review bodies help ensure that CSE policies and activities:

- are reasonable and necessary
- respect the privacy of Canadians and persons in Canada
- comply with the *CSE Act*, and all other Canadian laws
- are effective in meeting our mandate

This fiscal year, CSE contributed to 14 external reviews (12 by NSIRA and 2 by NSICOP). 4 reviews were initiated this fiscal year and 10 are ongoing.

To support their reviews, CSE provides both NSICOP and NSIRA with extensive access to information, documents, records, and subject matter experts.

Over the course of the fiscal year, CSE:

- dedicated thousands of hours to supporting external review
- responded to over 200 detailed questions from NSICOP and NSIRA
- provided access to tens of thousands of documents and records
- held over 20 briefings, meetings or interviews with review staff
- provided office space and building access to NSIRA for classified research
- proactively shared information about Ministerial Authorizations and Ministerial Orders with NSIRA

CSE values the important and independent review these bodies provide, as well as their recommendations on how to improve our policies and practices.

Improving processes to protect Canadian privacy

CSE is always looking for ways to improve our processes, especially when it comes to protecting the privacy of Canadians and persons in Canada.

CSE does not target Canadians or persons in Canada in our intelligence gathering. When Canadian Identifying Information (CII) is acquired incidentally, we make sure it is suppressed in our intelligence reporting to protect privacy. However, the clients who receive our reports can request the CII, as long as they have the legal authority to receive the information and the operational need to know.

In June 2021, NSIRA published a review of CSE's disclosures of CII.[91] The review made 11 recommendations to improve our processes for dealing with these requests.

Since the review began, CSE has completed 10 out of the 11 recommendations, including:

- performing 2 upgrades of enabling software
- improving the rigour of our disclosure processes
- creating additional requirements to document internal decisions and analyses
- engaging with client departments to clarify their legal authorities to receive the information

In addition, CSE completed a separate, internal study of our disclosure of CII to ensure our privacy measures are as robust as possible.

The final recommendation, to conduct a Privacy Impact Assessment (PIA) has been launched. We expect to complete the PIA in 2022.

The review also raised concerns that some disclosures of CII during the period of the review may have been non-compliant.

After detailed analysis of CSE's program, and the disclosures related to 2,351 Canadian identifiers cited in NSIRA's report, and following consultations with government partners, CSE is satisfied that all but one of those disclosures were compliant. The single disclosure that was not compliant with the *Privacy Act* has been retracted and the data that was disclosed has been purged by the receiving institution.

Reports by our oversight and review bodies

Our external oversight and review bodies publish unclassified annual reports and reviews where they share their findings with Canadians, helping to increase accountability and transparency.

The following reports relating to CSE were completed this fiscal year:

- Intelligence Commissioner
  - → Intelligence Commissioner Annual Report 2021[92]
- NSICOP
  - → Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack[93]
  - → NSICOP Annual Report 2020[94]
- NSIRA
  - → Review of the Communications Security Establishment's Disclosures of Canadian Identifying Information[95]
  - → Review Of Departmental Implementation Of The Avoiding Complicity In Mistreatment By Foreign Entities Act For 2019[96]
  - → NSIRA 2020 Annual Report[97]

Inspired **workforce**

Having a healthy, inspired workforce is at the heart of CSE's 2025 strategy. When our people are thriving, we deliver our mission for Canadians more effectively.

While CSE ranked highly in the most recent Public Service Employee Survey results,[98] we selected three priorities for workplace wellbeing in 2021:

- promoting equity, diversity and inclusion
- managing work-life balance, stress and mental health
- helping management and employees adapt to shifting "future of work" realities

Equity, diversity and inclusion

CSE's goal is to be a workplace where:

- our workforce reflects the diversity of the country we serve
- structural barriers that discriminate against marginalized groups are identified and removed
- inclusion is baked into our policies and practices
- no employee experiences harassment or discrimination
- we work towards reconciliation with Indigenous Peoples across Canada
- every employee is valued and celebrated for who they are

We are not there yet, but we are taking concrete steps towards that vision. From top-down changes to grassroots initiatives, below are some of the ways in which CSE has promoted equity, diversity and inclusion (EDI) this year.

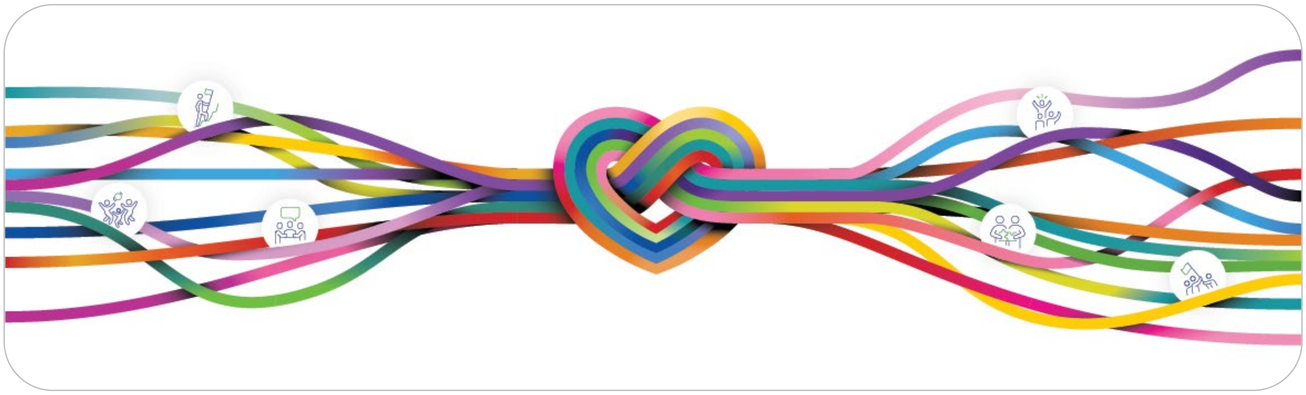
Senior advisor for EDI

In May 2021, CSE appointed a Senior Advisor for People, Equity, Diversity and Inclusion. Artur Wilczynski is a life-long advocate for equity, diversity and inclusion, and was, prior to his appointment, an Assistant Deputy Minister (ADM) in CSE's SIGINT branch.

Some of the ways the Senior Advisor has made an impact this year include:

- advising the Chief and Associate Chief on people-related issues
- working with activity areas to develop strategies that support people at the branch level
- supporting CSE's affinity groups (employee networks)
- building and maintaining relationships with:
  - → partners across Government
  - → external organizations
  - → Indigenous leaders
- working with CSE's Corporate Services Branch and Human Resources to focus on EDI in:
  - → recruitment and career development
  - → security screening renewals
  - → training
  - → facilities management
  - → self-identification for Employment Equity

> **As a person who arrived in Canada as a refugee facing ethnic persecution and as a Gay man, I understand what it means to be excluded. I know how much energy it saps from a person. I want all of us to dedicate all of our energy to our wellbeing and our shared vision for CSE. When we create a healthy, inclusive environment, we maximize our ability to deliver our mission.**
>
> **Artur Wilczynski**
> *ADM Senior Advisor for People, Equity, Diversity and Inclusion, CSE*



The Equity, Diversity, and Inclusion Framework

In March 2022, the People Committee approved the first ever Equity, Diversity and Inclusion Framework[99] for CSE. The framework sets ambitious goals to deliberately support EDI at CSE. It identifies ways to break down systemic barriers that get in the way of people's potential. It compels managers and employees to integrate diversity and inclusion at the operational level to make sure we meet the needs of all Canadians in carrying out our mission.

The framework was created in collaboration with employee affinity groups at CSE. It includes principles, strategies, and an action plan to make CSE a better place to work.

Affinity Groups

Initiatives such as the EDI Framework could not have been achieved without the insights and contributions of CSE's affinity groups. These groups are grassroots, employee networks that bring together colleagues with similar concerns around EDI. Everyone is encouraged to participate in any of the groups as a person with lived experience or as an ally.

This year, employee affinity groups at CSE:

- led initiatives to make CSE more inclusive
- contributed to new CSE policies
- created and shared guidance resources
- fostered safe spaces for mutual support
- organized speaker events and panel discussions
- hosted celebrations and commemorative events
- collaborated with advocacy groups at partner agencies
- delivered presentations and awareness sessions

Three new affinity groups launched this year:

- Disabilities
- EmbRACE (a support network for racialized employees and their allies)
- Neurodiversity

They join established employee networks, including:

- The Pride Network (representing Two Spirit, Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Asexual employees and allies)
- Women in Cyber and Intelligence (WICI)

> **The organization has already evolved from when we first started giving this presentation. There seems to be a genuine desire to learn and speak up from our senior management now.**
>
> **Jonathan Gohidé**
> *CSE employee, Being Black in Canada: An interview with CSE employees Jonathan and Marie*[103]

> **I find it has brought together the racialized and Indigenous employees at CSE (...) As we met more as a community, we came up with 8 action items that the organization could take to help our racialized employees. All the items have since been integrated in the Equity Diversity and Inclusion Framework, so areas of concern will be, and are being, addressed.**
>
> **Marie Calixte-McKenzie**
> *CSE executive*

Standing up to anti-Black racism

In February 2021, two CSE employees, Marie Calixte-McKenzie and Jonathan Gohidé, delivered their presentation, "Being Black in Canada", to a CSE all-staff event for Black History Month. They had written it to provide insight into what Black employees at CSE were experiencing after the murder of George Floyd.

The presentation had a profound impact. CSE asked Marie and Jonathan to deliver it to managers and executives and added a recording of the presentation to our mandatory training for new hires in July 2021.

The presentation inspired employees to form the EmbRACE affinity group, which held its first meeting in April 2021.

As of March 2022, Marie and Jonathan have delivered their presentation to over 36 groups, including:

- CSE employees, managers and executives
- CSE's UK counterpart, Government Communications Headquarters (GCHQ)
- the University of Ottawa's leadership program for senior public service executives
- over 2,600 public servants through the Federal Speakers' Forum[101] on Diversity and Inclusion

Reconciliation with Indigenous peoples

Reconciliation with Indigenous peoples is a core principle of CSE's new EDI Framework.

CSE executives are building relationships with local Indigenous leaders to listen to their experiences and to make sure our reconciliation efforts are culturally appropriate.

Cyber Centre executives are in discussions with Indigenous organizations to collaborate on cyber security outreach initiatives.

CSE is part of the Government of Canada IT Apprenticeship Program for Indigenous Peoples[102] and is exploring ways to encourage more Indigenous candidates to join CSE.

In June 2021, CSE organized an all-staff event to help employees understand the history and legacy of Canada's Indian Residential Schools system, in accordance with the Calls to Action by the Truth and Reconciliation Commission of Canada.

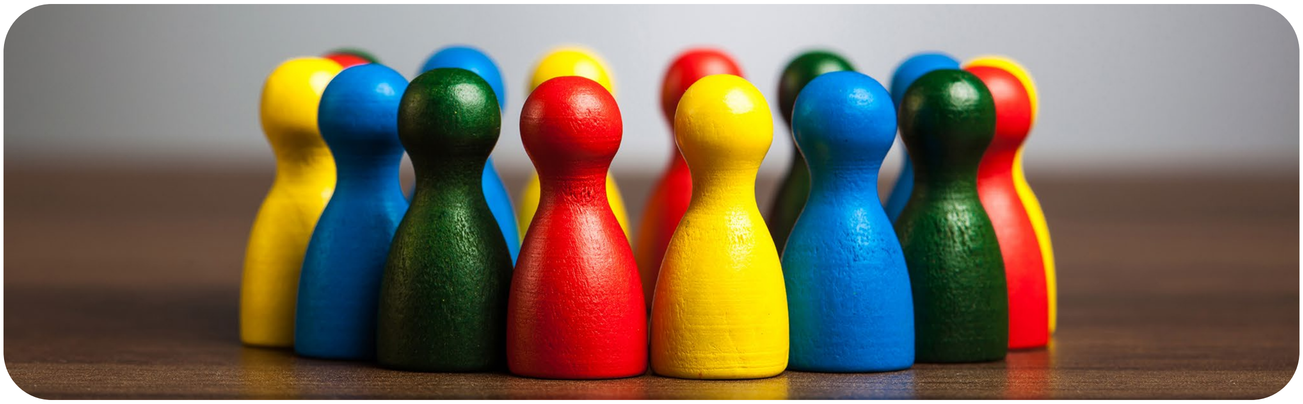
Reconciliation is not something that can be achieved overnight, but CSE is seeking out opportunities to advance it, step by step, in partnership with Indigenous peoples.

New guidance supporting transgender rights and gender diversity

In March 2022, CSE adopted a new guidance document: *Supporting transgender and gender diverse persons at the Communications Security Establishment*.[103] The document gives guidance to employees who may be transitioning or questioning their gender expression and identity about what they can expect from CSE as an employer. It also gives guidance to managers and colleagues on how best to support people through this process.

The guidance was created in consultation with members of CSE's Two Spirit, Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Asexual (2SLGBTQIA+) community. It will evolve along with laws and best practices.

> **Being an older transgender individual going through my transition, I needed to know how I would be accepted by both management and all CSE staff. Having a guide is a sort of insurance policy that would protect me from any possible negative reactions or hate that could be directed to me. It's not just for me. It's for all the younger people coming after me.**
>
> **Toni**
> *CSE employee, Making a difference by supporting transgender and gender diverse persons at CSE*[104]



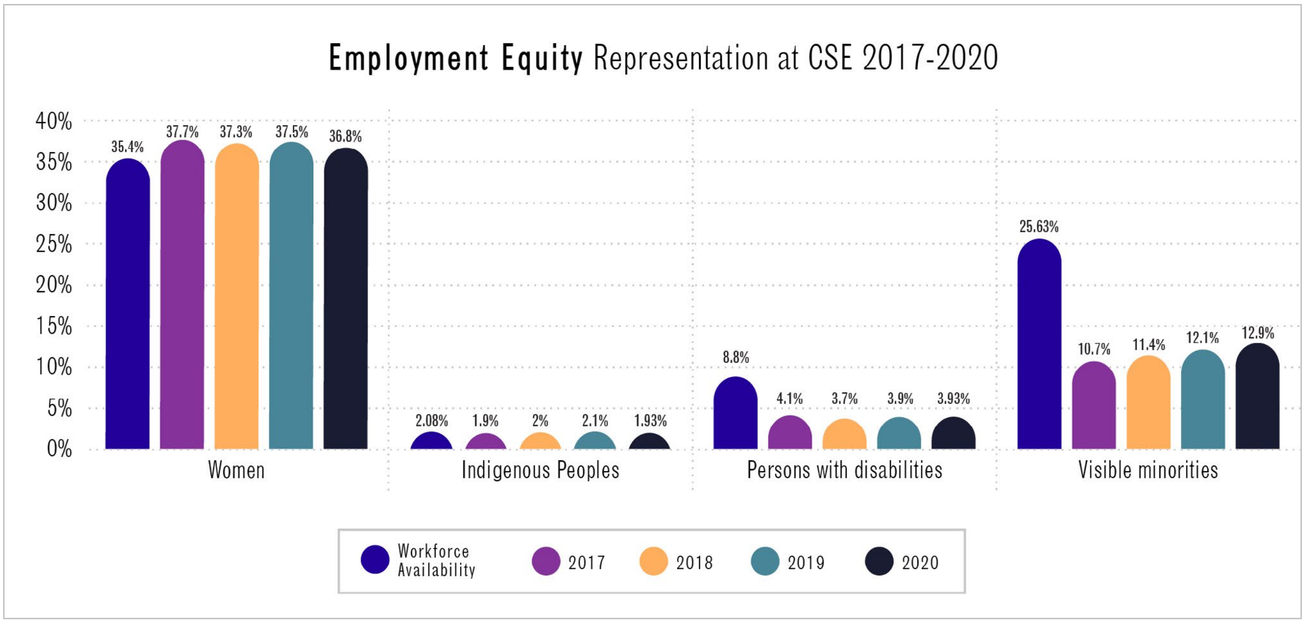
Employment Equity data

Under the Employment Equity Act, every government department and agency must gather data about its workforce. The aim of the act is to correct the disadvantages faced in the workplace by 4 designated groups:

- women
- Indigenous peoples
- members of visible minorities[105]
- persons with disabilities

CSE's most recent official Employment Equity (EE) statistics show that diversity is slowly increasing at CSE (see table below for 4-year trends up to 2020).[106]

CSE was not able to gather fresh EE statistics during the pandemic due to the unavailability of HR systems. However, in March 2022, CSE launched a new HR system which enabled us to started gathering new self-identification information. Early results show encouraging improvement in the representation of persons with disabilities (10%) as well as new statistics regarding the percentage of CSE individuals self-identifying as 2SLGBTQIA+ (5%). However, visible minorities and Indigenous individuals remain under-represented relative to their availability in the workforce. CSE is actively working to improve in these areas, as well as to increase the representation of women in STEM roles. We will be able to report fresh data in next year's annual report.


Employment Equity Representation at CSE 2017-2020

Self-Identification campaign

While the new HR system removed a logistical barrier to self-identifying, there were other barriers too. CSE consulted with employee affinity groups who relayed concerns about the process. Some employees had concerns about how the data would be used. Others expressed that the tick-box format did not accurately reflect their mixed heritage. Many said they had never self-identified to protect themselves from accusations of tokenism.

Based on that input, CSE designed a new in-house self-identification questionnaire and an internal communications campaign clarifying how the data is used and how it is not used (for example, it is not used in staffing or security processes). The campaign emphasized that more accurate data will help CSE identify and address gaps in representation.

The new HR system launched on March 1, 2022. By the end of the fiscal year about three-quarters of CSE employees had completed the self-identification. Once complete, the data will help CSE craft strategies to better reflect the country we serve.

> **To be honest, I used to have reservations about self-identifying because I wanted to make sure that if I was getting a job, it was because I was qualified for it, not just because I was a data point. Now, I really see the importance of this process and why we require this data as an organization – to measure where we are now and to track our progress moving forward. Every data point counts.**
>
> **Melanie Anderson**
> *CSE executive*

EDI online

Around 40% of employees are active on CSE's online discussion forums devoted to EDI. In addition to the affinity groups' channels, CSE has online communities dedicated to:

- Asian heritage
- Indigenous Peoples and reconciliation
- mental health
- official languages

In response to all the activity going on around these issues, in March 2022, CSE launched a dedicated EDI space on our internal website. It's a one-stop shop where employees can find resources, tools, policies, information about events and links to the affinity groups.

Official languages

CSE continues to make linguistic duality in the workplace a priority. As a heavily anglophone organization we are working to adapt our corporate culture to include more use of French in all places, at all levels. This is a long-term commitment supported by training and development. Employees are encouraged to speak in the language of their choice, while supporting those who are learning. All official communications, both internal and external, are presented in both official languages. This year CSE officially celebrated Linguistic Duality Day as well as International Francophonie Day.

In September 2021, CSE launched an internal tool to help management determine language requirements for positions. This interactive tool presents a series of questions related to the functions performed by a position's incumbent which leads to a logical, consistent, and objective result.

CSE also introduced a Linguistic Risk-Taking Passport, available in both English and French. The passport features a checklist of challenges to encourage CSE language learners to practice their skills in real-life situations.

All-staff events

CSE holds regular all-staff events (virtually for now) featuring internal and external speakers. This year, many of the all-staff events related to EDI themes, including:

- anti-bullying and harassment
- dyslexic thinking skills
- EDI at CSE
- empowering young women and girls in tech
- gender identity and gender expression
- Holocaust Remembrance Day
- National Accessibility Week
- Reconciliation with Indigenous peoples

Recruitment

Over the past year, CSE has modernized its recruitment process to make it more user-friendly, transparent and interactive. We have bolstered our efforts to recruit more diverse candidates by:

- removing gender-biased language from job descriptions
- promoting diversity and inclusion in our recruitment materials
- attending recruitment events that focus on underrepresented groups
- providing interview training to hiring managers
- proactively reaching out to potential candidates on professional social media networks
- liaising with:
  - → Indigenous groups
  - → groups that promote women in tech careers

Employee wellbeing

The pandemic has been tough on everyone, mentally, physically and emotionally. Here are some of the ways CSE has worked to support our employees this year.

Mental health

All CSE employees have access to in-house professional counselling, so they can talk freely about anything, even if it is classified. Our Employee and Organizational Wellness (EOW) program includes:

- the Counselling and Advisory Program (CAP)
- the Disability Management Program
- Career Transition services

Since the onset of the pandemic, employees have been able to access these services either on-site or virtually.

This year CAP designed and delivered training sessions that were open to all employees, including:

- managing anxiety
- parenting during the pandemic
- working from home
- self-compassion
- returning to work on site

CAP continued to run weekly meditation sessions online in both French and English.

CSE also encouraged employees to take advantage of mental health resources from the Canada School of Public Service including webcasts, training courses and virtual events.

> **Thanks. I find that these kinds of conversations and courses - with the questions that come up and the input from others - have the effect of making me realize what is really going on with me and how I'm really feeling about the current situation and what's coming up. It's tough to face, but helpful.**
>
> **CSE employee feedback**

Harassment and Violence and Prevention Program (HVPP)

In January 2021, CSE expanded its capacity for preventing and handling incidents of harassment and violence at work in line with new federal legislation.[107]

The new Harassment and Violence Prevention Program (HVPP) is staffed by 4 advisors (up from 1 in 2020).

As well as providing a safe space for reporting incidents, the HVPP Office now also focusses on prevention. In line with the new legislation, the HVPP Office also extends support to employees who are victims of domestic violence.

This year, the HVPP Office provided:

- support to affected parties through the resolution process
- help with workplace assessments
- risk mitigation measures
- emergency procedures
- support to employee victims of domestic violence
- prevention strategies
- information sessions
- training resources
- information about support services in the community

Harassment and violence prevention training is now mandatory for all CSE employees.

COVID-19 protocols

The details of CSE's COVID protocols changed many times this year, adjusting up and down as the waves came and went. However, the overall principle was to ensure a safe working environment for our on-site staff while maintaining operations. For example, we kept masking and physical distancing requirements on site even when these were no longer required by local health directives.

The cautious approach was to protect our employees' physical health, but also to minimize anxiety for those whose classified work can only be done on site.

In January 2022, CSE began a COVID-19 Rapid Test program in partnership with Health Canada. Employees working on site could opt to take rapid antigen tests three times a week. Although voluntary, participation was strong. The data was anonymized before being sent to Health Canada.

All changes to our COVID approach were communicated clearly ahead of time through regular staff emails and a digital guidebook that was kept up to date.

Preparing for the future of work

The pandemic has changed a lot of our assumptions about what a workplace is. CSE is adapting to take advantage of new technologies and ways of working.

Telework agreements

Over the past two years, CSE's workforce has been split into two categories. Those whose work is classified (such as SIGINT employees) have continued to work at our secure facilities, with appropriate public health measures in place. Anyone who could work from home, did.

There are advantages and disadvantages to both modes of working. As we move forward, the aim is to keep the best of both worlds, while minimizing the downsides.

In the fall of 2021, CSE began a gradual return to the office for employees who had been working from home. CSE gave the option of teleworking part-time to employees whose duties can be performed remotely. We planned to begin a one-year trial period for this hybrid approach in January 2022. It was pushed back to April 2022 due to the arrival of the Omicron variant.

Supporting distributed teams

CSE has set up a dedicated space on our internal website to support distributed teams. Resources included:

- guidance for managers of distributed teams
- a CSE Work from Home Guidebook for employees
- security tips for organizations with remote workers
- links to training sessions
- articles
- Government of Canada job aids

Multi-classification environment

In the past, CSE's IT systems operated only on the "high side" (a secure environment for information classified Secret and above).

That changed with the formation of the Cyber Centre in 2018, which works primarily on the "low side" to facilitate collaboration with outside partners.

Then in 2020, the picture became more complicated with the need for secure remote working during the pandemic. As described in last year's report, this was made possible by the extraordinary efforts of our technology services team who quickly deployed devices and enabled new capabilities for working securely from home.

Partly by design, partly out of necessity, CSE has fully embraced working in a multi-classification environment. This year, we have continued to build and maintain new IT infrastructure. We have come up with new ways to properly secure and safeguard devices, sharing our lessons learned with other Government of Canada departments. We have made big shifts in how we classify and manage information. We have established new tools for collaborating across classification levels. All of this required careful planning, as well as training and awareness for employees.

Migrating to the cloud

CSE continues to act as a pathfinder for the Government of Canada in migrating to the cloud. We were the first department to securely implement several commercial cloud applications, securing them with our cloud-based sensors and sharing the lessons learned with other departments. Over the past year, CSE has continued to shift low-side workloads, services, tools and applications to the cloud. This shift allows CSE to deploy new tools more quickly and allows our employees to work and collaborate more easily.

Top Employer

In January 2022, CSE was recognized as one of Canada's Top Employers for Young People[108] for the 6th year in a row. CSE was also named one of the National Capital Region's Top Employers [109]for the 7th time in 10 years (2013, 2014, 2015, 2018, 2020, 2021 and 2022).

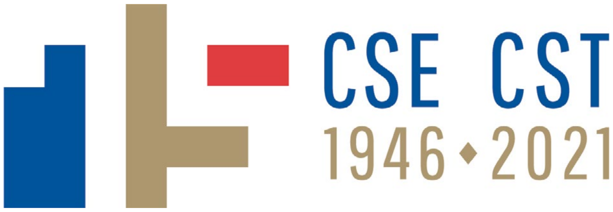
The selection process is overseen by the editors of Canada's Top 100 Employers publication. The criteria include:

- physical workplace
- work atmosphere
- health, financial and family benefits
- training and skills development
- community involvement

CSE is hiring. Visit our careers page.[110]

CSE's 75th anniversary

September 1, 2021, marked CSE's 75th anniversary. The event gave us a chance to give Canadians a glimpse into our day-to-day work over the decades.



Sharing our story

We expanded our external History web pages[111] by creating a special 75th anniversary[112] section. This content included a series of vignettes[113] on topics, people, places, objects and events that played a major role in our history. We also included stories from our wartime predecessor organizations, the Examination Unit (civilian) and the Joint Discrimination Unit (military).

CSE was privileged to include many former Chiefs in our celebrations. The 6 most recent Chiefs joined current Chief Shelly Bruce to commemorate CSE's milestone anniversary by reflecting on the highlights and challenges of leading the organization during their terms, stretching from the end of the Cold War to the present day:

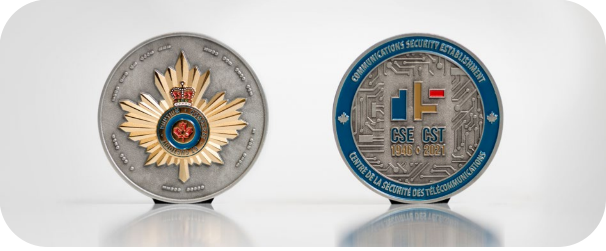
- Stewart Woolner (1989 to 1999)
- Ian Glen (1999 to 2001)
- Keith Coulter (2001 to 2005)
- John Adams (2005 to 2012)
- John Forster (2012 to 2015)
- Greta Bossenmaier (2015 to 2018)
- Shelly Bruce (2018 to present)

We shared much of our anniversary content on social media, including a new CSE history post every day for 75 days leading up to September 1, 2021.

Logo and Challenge Coin

CSE developed a unique CSE 75 logo for use in our anniversary projects. The logo was featured on one side of a special CSE 75 challenge coin, designed in-house and distributed to special guests.

The logo itself is a small puzzle, consisting of red, gold and blue blocks (the colours of the CSE badge) with the number "75" visible in the white space between.


COMMUNICATIONS SECURITY ESTABLISHMENT
CSE CST
1946 • 2021
CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

CSE 75 Special Event Station

Morse code and ham radio played vital roles in the development of signals intelligence capabilities and were some of the earliest technologies used during our formative years.

CSE employees with ham radio licenses worked with CSE's history program to set up a radio station on the lawn of the Edward Drake Building, registered under the special event callsigns VE3CSE75 and VE3CST75.

The station was announced[114] on our social media platforms and operated on both continuous wave (Morse code) and voice (phonetic alphabet) channels for two days in October 2021.

CSE's Chief, Shelly Bruce, officially opened the event the morning of October 27 and connected directly with our UK counterparts at GCHQ. By the end of the special event, our station had made over 450 contacts across 34 countries.

CSE at a **glance**

- The current Chief of CSE is Shelly Bruce
- The Chief reports to the Minister of National Defence, the Honourable Anita Anand
- CSE’s 2021 to 2022 budget is $859 million, total authorities
- Our workforce is 3199 full-time employees

Key dates

1939–1945
Canadian military and civilian units provide signals intelligence during the Second World War

1946
Canada establishes the Communications Branch of the National Research Council

1975
The agency is renamed the Communications Security Establishment and moved under National Defence

2011
CSE becomes a standalone agency reporting to the Minister of National Defence

2018
Canada establishes the Canadian Centre for Cyber Security within CSE

2019
The CSE Act comes into force

2021
CSE marks 75 years of protecting Canada and Canadians

Endnotes

1 https://cyber.gc.ca/en/

2 https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent#ID0EGTCK

3 https://pm.gc.ca/en/mandate-letters/2021/12/16/minister-national-defence-mandate-letter

4 https://www.cse-cst.gc.ca/en/mission

5 https://cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion

6 https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators

7 https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html

8 https://www.cse-cst.gc.ca/en/information-and-resources/news/cse-statement-threat-activity-targeting-covid-19-vaccine-development

9 https://www.cse-cst.gc.ca/en/information-and-resources/announcements/cse-statement-malicious-russian-cyber-activity-targeting

10 https://www.cse-cst.gc.ca/en/information-and-resources/news/cse-statement-notpetya-malware

11 https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html

12 https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html

13 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadian-critical-infrastructure-operators-raise

14 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators

15 https://cyber.gc.ca/en/cyber-threats-canadas-democratic-process-july-2021-update

16 The table is for the calendar year to be consistent with our review bodies. Other references to "this year" still refer to the fiscal year.

17 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

18 https://cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp

19 https://cyber.gc.ca/en/tools-services/common-criteria

20 https://cyber.gc.ca/en/guidance/using-encryption-keep-your-sensitive-data-secure-itsap40016

21 https://cyber.gc.ca/en/news-events/host-based-sensors

22 National Security and Intelligence Committee of Parliamentarians, *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack*, February 2022

23 https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf

24 https://cyber.gc.ca/en/glossary

25 https://cyber.gc.ca/en/guidance

26 https://www.gov.nl.ca/hcs/information-and-updates-on-cyber-incident/

27 https://cyber.gc.ca/en/tools-services/assemblyline

28 https://cybercentrecanada.github.io/assemblyline4_docs/

29 https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html

30 https://pm.gc.ca/en/news/statements/2021/02/23/roadmap-renewed-us-canada-partnership

31 https://www.cga.ca/cyber-security/

32 https://www.ieso.ca/en/Sector-Participants/Cybersecurity/Sector-Services---Lighthouse

33 https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector

34 https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021#support

Endnotes

[35] https://lih-cai.cse-cst.gc.ca/login/index.php

[36] BC Chamber of Commerce, *Cyber Security and Business Survey*, https://bcchamber.org/wp-content/uploads/2021/10/Cyber-Security-and-Business-Survey-Summary-Report.pdf (English only)

[37] https://cyber.gc.ca/en/guidance/cyber-security-resources-small-and-medium-organizations-itsap00137

[38] https://cyber.gc.ca/en/incident-management

[39] https://www.cira.ca/cybersecurity-services/canadian-shield

[40] https://cyber.gc.ca/en/cyber-threats-canadas-democratic-process-july-2021-update

[41] https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-operational-technology

[42] https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-ransomware-threat-2021

[43] https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-reminds-canadian-critical-infrastructure-operators

[44] https://cyber.gc.ca/en/publications

[45] https://www.cyber.gc.ca/en/ransomware

[46] https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

[47] https://www.cyber.gc.ca/en/guidance/digital-footprint-itsap00133

[48] https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005

[49] https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100

[50] https://cyber.gc.ca/en/guidance/strategies-protecting-web-application-systems-against-credential-stuffing-attacks

[51] https://cyber.gc.ca/en/guidance/security-considerations-industrial-control-systems-itsap00050

[52] https://cyber.gc.ca/en/guidance/protect-your-medical-research-equipment-cyber-threats-itsap00134

[53] https://cyber.gc.ca/en/guidance/cyber-security-connected-medical-devices-itsap00132

[54] https://cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300

[55] https://cyber.gc.ca/en/guidance/securing-access-controls-volunteer-based-organization-itsm30010

[56] https://www.cyber.gc.ca/en/guidance/security-considerations-electronic-poll-book-systems-itsm10101

[57] https://cyber.gc.ca/en/guidance/security-considerations-when-using-social-media-your-organization-itsm10066

[58] https://cyber.gc.ca/en/news/joint-cybersecurity-advisory-mitigating-log4shell-and-other-log4j-related-vulnerabilities

[59] https://www.cyber.gc.ca/en/alerts/active-exploitation-apache-log4j-vulnerability

[60] https://www.getcybersafe.gc.ca/en/resources/celebrating-10-years-get-cyber-safe

[61] https://www.getcybersafe.gc.ca/en/blogs/be-prepared-how-your-business-can-protect-itself-ransomware-attacks

[62] https://www.getcybersafe.gc.ca/en/blogs/ransomware-101-how-stay-cyber-secure

[63] https://www.getcybersafe.gc.ca/en/resources/video-malware-and-ransomware

[64] https://www.getcybersafe.gc.ca/en/resources/ransomware-back-your-data-or-else

[65] https://www.getcybersafe.gc.ca/en/resources/cyber-security-checklist

[66] https://www.getcybersafe.gc.ca/en/blogs/how-older-adults-can-protect-themselves-most-common-cyber-security-threats

[67] https://www.getcybersafe.gc.ca/en/resources/real-examples-fake-emails

[68] https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-protect-your-time-online

[69] https://www.getcybersafe.gc.ca/en/blog/cyber-threats-families-watch-out-for

[70] https://www.getcybersafe.gc.ca/en/resources/whats-your-cyber-security-backpack

[71] https://www.getcybersafe.gc.ca/en/blogs/how-avoid-sharing-too-much-information-online

[72] https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-agency

[73] https://www.getcybersafe.gc.ca/en/resources/get-cyber-safe-gift-guide

74 https://www.getcybersafe.gc.ca/en/resources/video-festive-yule-firewall-2021

75 https://getcybersafe.gc.ca/en/resources/gingerbread-home-network-kit

76 https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month

77 https://www.getcybersafe.gc.ca/en/resources/csam-resources

78 https://learning-apprentissage.ised-isde.canada.ca/course/index.php?categoryid=52

79 https://cyber.gc.ca/en/certifications-field-cyber-security-2020

80 https://cyber.gc.ca/en/guidance/appendix-b-post-secondary-cyber-security-related-programs

81 https://cse-cst.gc.ca/en/culture-and-community/community-engagement#community

82 https://cse-cst.gc.ca/en/culture-and-community/research/tutte-publications-and-events#events

83 https://cyber.gc.ca/en/guidance/addressing-quantum-computing-threat-cryptography-itse00017

84 https://https-everywhere.canada.ca/en/index/

85 https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html

86 https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021

87 https://www.cse-cst.gc.ca/en/accountability/transparency/proactive-disclosure

88 https://www.cse-cst.gc.ca/en/accountability/transparency/access-information-and-privacy-atip

89 https://open.canada.ca/en/search/ati?f%5B0%5D=ss_ati_organization_en%3ACommunications%20Security%20Establishment&ati%5B0%5D=ati_organization_en%3ACommunications%20Security%20Establishment%20Canada

90 This table is for the calendar year to be consistent with our review bodies.

91 https://nsira-ossnr.gc.ca/review-of-the-communications-security-establishments-disclosures-of-canadian-identifying-information

92 https://www.canada.ca/content/dam/oic-bcr/documents/ICO-Annual Report-2021.pdf

93 https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-en.html

94 https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html

95 https://nsira-ossnr.gc.ca/nsiras-review-of-cses-disclosures-of-canadian-identifying-information-cii

96 https://nsira-ossnr.gc.ca/review-of-departmental-implementation-of-the-avoiding-complicity-in-mistreatment-by-foreign-entities-act-for-2019

97 https://nsira-ossnr.gc.ca/tabling-of-the-national-security-and-intelligence-review-agencys-annual-report

98 https://www.tbs-sct.canada.ca/pses-saff/2020/results-resultats/en/bt-pt/org/89

99 https://cse-cst.gc.ca/en/culture-and-community/diversity-inclusion/one-cse-framework-equity-diversity-and-inclusion

100 https://www.cse-cst.gc.ca/en/being-black-canada-interview-cse-employees-jonathan-and-marie

101 https://tbs-blog.canada.ca/en/marie-calixte-mckenzie-and-jonathan-gohide-being-black-canada

102 https://alfdc.on.ca/wp-content/uploads/2021/10/GCITApprenticeship-Poster-E.pdf

103 https://www.cse-cst.gc.ca/en/supporting-transgender-and-gender-diverse-persons-communications-security-establishment

104 https://www.cse-cst.gc.ca/en/making-difference-supporting-transgender-and-gender-diverse-persons-cse

105 CSE recognizes that this term is considered outdated. We use it here in the context of the *Employment Equity Act*, which is currently under review. https://www.canada.ca/en/employment-social-development/corporate/portfolio/labour/programs/employment-equity/task-force.html

106 Note: The CSE data represents information voluntarily disclosed by our employees under the Government's self-identification program, as required by the *Employment Equity Act*. Workforce availability reference levels are based on Labour Market Availability census data (2016), factoring in additional criteria: citizenship, location and National Occupational Classification code comparisons.

107 https://gazette.gc.ca/rp-pr/p2/2020/2020-06-24/html/sor-dors130-eng.html

Endnotes

[108] https://reviews.canadastop100.com/top-employer-communications-security-establishment#young

[109] https://reviews.canadastop100.com/top-employer-communications-security-establishment

[110] https://cse-cst.gc.ca/en/careers

[111] https://www.cse-cst.gc.ca/en/culture-and-community/history

[112] https://www.cse-cst.gc.ca/en/culture-and-community/history/75th-anniversary

[113] https://www.cse-cst.gc.ca/en/culture-and-community/history/75th-anniversary/cse-75-vignettes

[114] https://twitter.com/cse_cst/status/1452697928808681472