Government of Canada / Gouvernement du Canada

Communications Security Establishment Annual Report 2020-2021

From: Communications Security Establishment Canada

ISSN 2564-047X

▶ Table of contents

Foreword from the Minister of National Defence

The Communications Security Establishment (CSE) might not be the first government agency you would think of in relation to a global health emergency, but the shift to virtual brought on by COVID-19 put foreign

intelligence, cyber security and information assurance right at the heart of Canada's pandemic response.

For CSE, as for the rest of Canada, 2020-2021 has been a time of both unprecedented challenges and hard-won achievements. From helping government to operate securely online and providing vital information to decision-makers, to defending the vaccine rollout from cyber threats, CSE's work has been a critical part of Canada's whole-of-government approach.

CSE has also been at the forefront of protecting Canadian individuals and organizations from cyber actors looking to exploit the pandemic to extort money, spread disinformation, steal personal data or copy intellectual property.

This report provides a snapshot of the scope and depth of those contributions.

As Minister of National Defence, I commend CSE for its technical leadership and innovation, operational agility and sheer hard work over the last 12 months. Canadians are safer because of your efforts.

- The Honourable Harjit S. Sajjan, Minister of National Defence.

One CSE: A message from the Chief

I began my career at CSE 32 years ago, and I learned early on, that in the security and intelligence business, organizations like CSE don't take curtain calls. We are used to promoting and defending Canada's interests from behind the scenes.

But things are changing. Cyber security is becoming more and more integral to the lives of Canadians. Emerging technologies are disrupting the status quo. New foreign adversaries are emerging; familiar ones are evolving. Canadians, quite rightly, are demanding more transparency from their government institutions than ever before. And in response, CSE is learning to raise the curtain on our activities a little more, and even, sometimes, to take centre stage.

In this year of the COVID-19 pandemic, CSE's mission became important in ways we never imagined, and our community went above and beyond to deliver important results for Canada.

With this annual report, we will shine a spotlight on some of those contributions.

The COVID-19 response

In early 2020 we wrote our strategic vision for the next five years: CSE 2025. Central to that vision is the principle of **One CSE:** "CSE effectively integrates all aspects of its mandate as Canada's national cyber leader."

When the pandemic hit, CSE 2025 served as our compass through uncharted territory. And in the spirit of One CSE, we pulled together as a community, bringing the various elements of our mandate to bear in support of the government's response, from cyber security and information assurance, to foreign signals intelligence.

We identified, blocked and responded to new cyber threats directed at government, the health sector and other critical Canadian systems, including the current vaccine rollout.

We delivered highly actionable foreign intelligence to our government clients.

We helped Cabinet, parliamentary and government business to operate more securely online.

We mitigated serious new cyber risks by alerting Canadians and Canadian businesses, offering guidance and support, and promoting best cyber security practices.

We found new and innovative ways to package intelligence and reach distanced government clients.

We helped the government accelerate and secure its transition to the cloud and bolster online security for its services to Canadians.

We provided thought-leading technical input and stress-tested proposed solutions.

And all of this happened on top of CSE's regular business, with only a fraction of our staff able to access our secure facilities at a time.

I have been impressed and humbled every day by the technical wizardry, the operational flexibility, and the positive mindset with which CSE employees approached the many curveballs the pandemic sent our way. I hope this report will give Canadians a sense of the breadth and the significance of those achievements. They really are worth celebrating.

Systemic inequities

However, as we take stock of the last year, it is important to note that COVID-19 also exposed long-standing inequities in Canada's society and institutions, from which CSE is not immune.

In this context **One CSE** has taken on new significance, to mean a workplace where everyone belongs, where there are no barriers to participation, and where the experiences and perspectives of our decision-makers faithfully reflect the diversity of the country we serve. Not just because it's the right thing to do (though, of course, it is) but because it will help us deliver our mission for Canadians more effectively. The different perspectives, skills, talents and experiences of multi-disciplinary teams are the best way, sometimes the only way, to solve intractable problems. This has been the central tenet of our success for three-quarters of a century.

Because we consider diversity to be an operational imperative for CSE, we have prioritized it for the best part of a decade. But I will be the first to admit that the pace of change has not been fast enough, and that we need to do more. The events of the past year have served as a stark reminder that progress is not inevitable. Systemic inequities don't fix themselves.

Therefore, in full agreement with the call to action on anti-racism from the Clerk of the Privy Council, CSE employees and executives entered 2021 determined to listen, to learn, and to act, beginning with a hard look at our policies and practices. It will take concerted effort to remove barriers for under-represented groups and to deliberately level the playing field where it needs levelling. The way CSE employees, managers and executives have set their problem-solving brains to that challenge fills me with hope for the future.

And so, as I reflect on the events of the past 12 months, am I keen to see the back of this wretched pandemic? Absolutely and unequivocally, yes.

But at the same time, am I excited to use the lessons we have learned to shape the next iteration of CSE? One hundred per cent.

And am I proud of what we have achieved for Canada this past year as an organization, as a community, and as **One CSE**?

Proud doesn't even begin to cover it.

Shelly Bruce
Chief, CSE

About this report

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

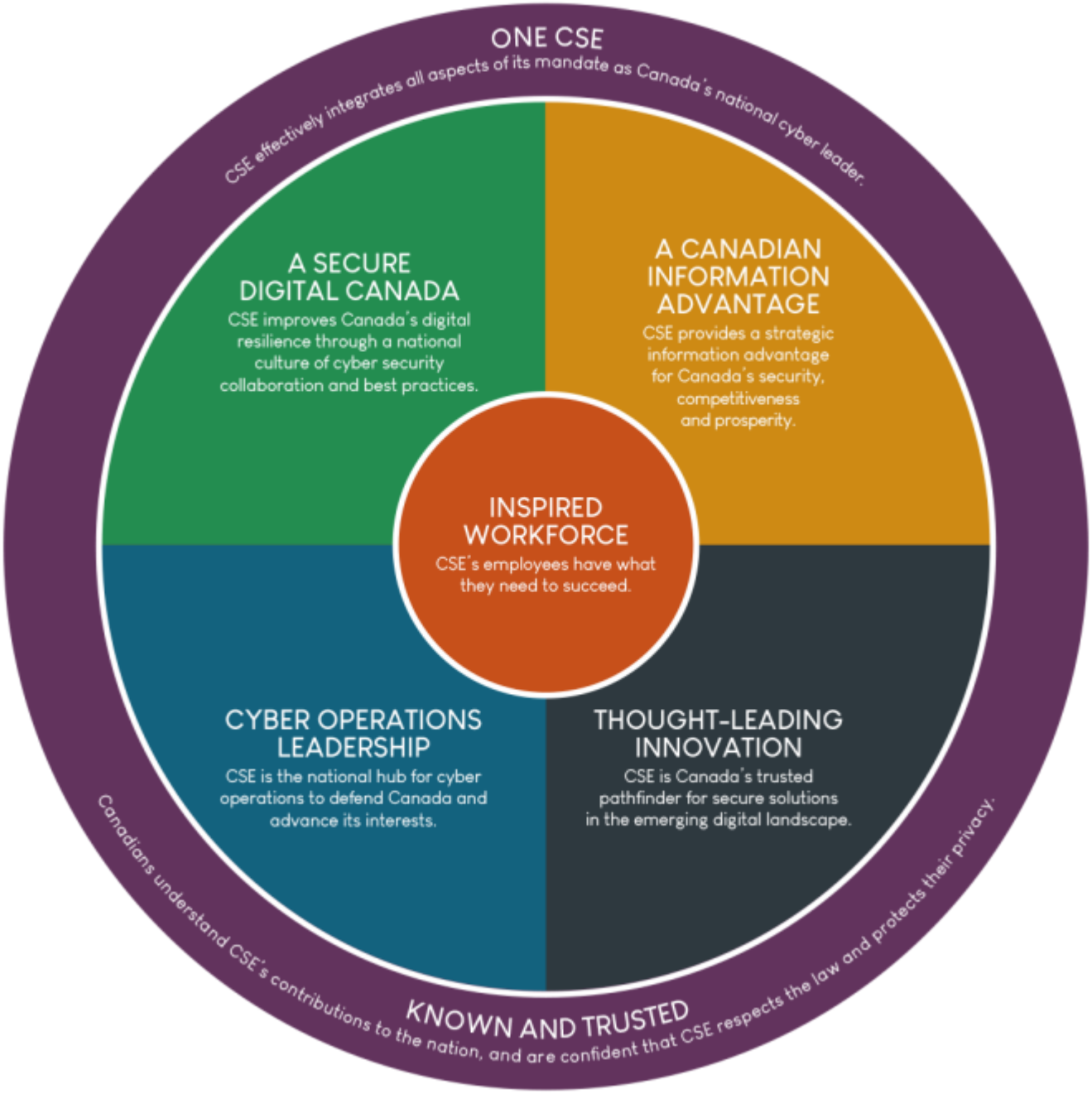
The Canadian Centre for Cyber Security (Cyber Centre), is a part of CSE. It was stood up in 2018, combining cyber expertise from across the federal government and is the operational lead for cyber security.

This report is unclassified. It does not contain operational details about our foreign signals intelligence or foreign cyber operations activities, because their effectiveness depends upon our adversaries not knowing how we do what we do. However, it does give examples of some of the ways those activities have benefitted Canada over the past year. We are free to report in more detail about the public-facing activities of CSE's Cyber Centre.

With the exception of "Supporting Canada's COVID-19 response" the chapter headings of this report follow the themes of our five-year strategic framework, CSE 2025.

The report aims to show how our activities over the past year deliver on that strategy.

The reporting period is April 1, 2020 to March 31, 2021. Unless otherwise noted, statistics and references to "this year" correspond to the fiscal year.



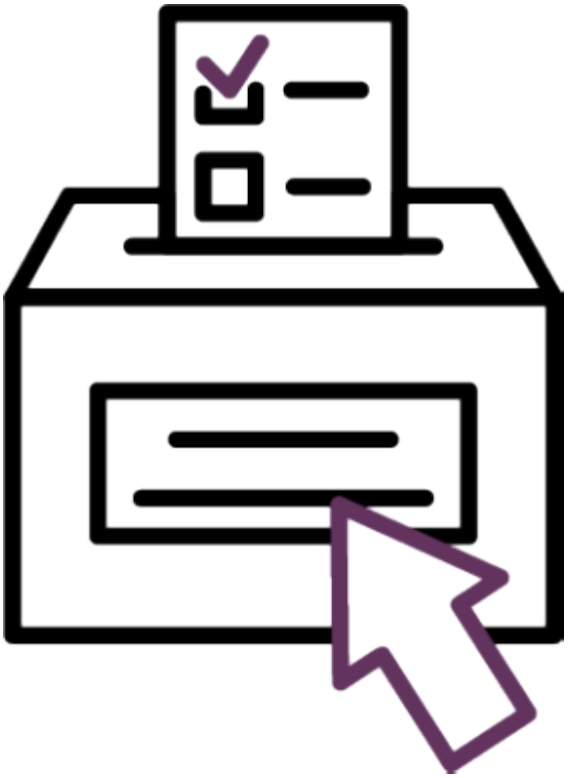
▶ Long description - CSE's 5-year strategic roadmap: CSE 2025

Supporting Canada's COVID-19 response

The need for physical distancing due to COVID-19 meant secure communications, cyber security and timely foreign intelligence were fundamental to Canada's pandemic response. CSE teams created new tools, new services and new partnerships to protect government operations, individual Canadians, the health sector and the vaccine response from cyber threats.

Protecting and enabling the government response

From the beginning of the pandemic, the Cyber Centre's secure communications solutions enabled Cabinet to lead the federal government response without having to meet in person. Ministers and senior officials could communicate at a classified level using commercial mobile handsets. The Cyber Centre also partnered with Shared Services Canada and the Privy Council Office to design and deliver a classified video-conferencing service for use by Cabinet and senior officials. This was completed and began operation in February 2021.

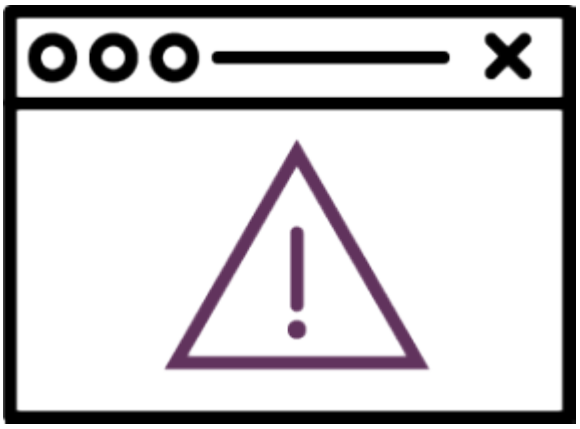


In April 2020, the Cyber Centre helped the House of Commons set up video-conferencing so that parliamentary business could continue. And in March 2021, Canadian Members of Parliament (MPs) voted for the first time using a secure virtual voting app, developed by the House of Commons, with technical input from the Cyber Centre. The app uses facial recognition technology and multi-factor authentication to verify MPs' identities.

As Government of Canada agencies and departments migrated rapidly to the cloud, we shared best practices to accelerate that shift and deployed innovative tools to keep their networks secure. For example, the Cyber Centre deployed cloud-based sensors to more than 50 departments (39 of them in this fiscal year) to help detect malicious cyber activity on their cloud infrastructure.

CSE experts also conducted vulnerability assessments and stress-testing of the COVID Alert (exposure notification) app to make sure it met the strict standards of privacy and security that Canadians have the right to expect.

Protecting Canadians



Cyber threat actors never let a crisis go to waste. They quickly pivoted to using COVID-19 themed phishing lures and fraudulent websites to try to scam Canadians. Among the most frequently impersonated government websites and email addresses were the Public Health Agency of Canada, Canada Border Services Agency, Canada Revenue Agency, and domains related to the Canada Emergency Response Benefit (CERB). From the start of the pandemic to the end of March 2021, CSE worked with trusted commercial and international partners to take down over 7,000 of these fraudulent domains.

Protecting Canada's health sector

Within a week of the nationwide shutdown in March 2020, the Cyber Centre alerted Canada's health sector that it faced an elevated risk from cybercriminals seeking ransoms, and from state-sponsored groups looking to steal COVID-19 research and sensitive data. This prediction was borne out by events, and we followed up in May 2020 with targeted advice for COVID-19 research and development organizations.

Over the past year, the Cyber Centre established new partnerships with over 100 health sector organizations, including provincial and territorial regional health authorities, patient care facilities, and organizations involved in the development, manufacture and delivery of COVID-19 vaccines.

The Cyber Centre issued over 20 cyber alerts to health sector partners and provided incident response support in more than 85 cases affecting the sector.

Throughout 2020 the Cyber Centre held weekly video calls with over 100 representatives from the health sector to share practical advice and answer questions about cyber threats. In 2021, these calls are continuing on a bi-weekly basis.

Protecting the vaccine rollout

The more vital something is, the more appealing a target it becomes for cyber attackers seeking to extract ransoms or cause disruption. Canada's COVID-19 vaccine rollout is just such a target.

In January 2021, the Cyber Centre began working with the Public Health Agency of Canada's National Operations Centre to bolster the cyber security of vaccine suppliers, warehouses, hospitals and vaccine administration sites across Canada. This included:

- reinforcing network perimeter security and access control
- updating, patching and securing devices connected to the Internet
- safeguarding stored vaccination data
- raising staff awareness of cyber threats

In March 2021, the Cyber Centre's Learning Hub worked with the Ontario Provincial Police (OPP) to develop and deliver a COVID-19 Cyber Threat Awareness course to be shared across Canada with health care workers, technicians and administrators involved in the COVID-19 vaccine deployment.

A live weekly training session and an on-demand recorded version launched in April 2021, led by Cyber Centre and OPP instructors. The Public Health Agency of Canada shared the course via their networks with the 300 vaccination sites across Canada.

Delivering key insights

Throughout the pandemic, CSE's foreign signals intelligence (SIGINT) mandate supported the federal government by providing Canadian decision-makers with key insights into international readiness and foreign reactions, to inform Canada's pandemic response.

SIGINT analysts identified foreign cyber threat activity aimed at Canada's health sector and notified our cyber defence teams so they could take action to block it.

CSE identified foreign cyber espionage targeting COVID-19 vaccine research and worked with our allies to attribute that behaviour publicly.

CSE SIGINT also identified foreign disinformation campaigns seeking to undermine trust in Canadian public health guidance and the safety and efficacy of COVID-19 vaccines. By alerting government clients, such as the Public Health Agency of Canada, to these campaigns, CSE classified reporting informs their public awareness efforts to counter these false and harmful narratives.

During this time, CSE reinvented the way we package intelligence reports to provide critical information about the pandemic more quickly, and in a more digestible format. We also adjusted our dissemination approach to be able to securely deliver timely intelligence to a wider group of government clients, including clients working remotely.

Cyber operations leadership

CSE is the Government of Canada's operational lead for cyber security. While much of that effort over the past year focused on the pandemic response, our regular work defending Canada and advancing its interests continued and intensified.

Protecting the gc.ca

Praise for HBS from our UK partners:

"We'd like to take this opportunity to thank the Canadian Centre for Cyber Security for all their help and support in enabling us to get to this point. The NCSC would not have been able to take on this challenge alone.

As if this weren't enough, the lessons we've learned protecting endpoint devices has helped us to defend our Health Sector during the COVID crisis."

- National Cyber Security Centre, UK

CSE is responsible for protecting Government of Canada networks, systems and databases from cyber threats. Our world-class dynamic defence capability routinely blocks between 2 and 7 billion malicious actions every

day, helping to protect services Canadians rely on, and keeping their personal information secure. On a particularly busy day, that figure can be closer to 10 billion.

In November 2020, CSE revealed part of the secret sauce behind that defence capability: host-based sensors (HBS). Developed in-house by CSE experts over the course of several years, HBS is now installed on over 700,000 Government of Canada endpoints (such as laptops, desktops and servers), where it automatically detects and neutralizes malicious activity, like malware trying to download. Each sensor securely gathers system data, while protecting the privacy of those using the service.

We are proud of the leading-edge nature of HBS. In November 2020, our UK counterparts at the National Cyber Security Centre officially thanked the Cyber Centre for allowing them to use HBS technology, saying it has "transformed (their) ability to detect threats and defend the UK government in cyberspace."

Protecting critical infrastructure

CSE's Cyber Centre cultivates strategic partnerships with Canadian critical infrastructure owners and operators to share knowledge and to co-develop new cyber security solutions.

In 2020-2021 the Cyber Centre forged new partnerships in 16 critical infrastructure sectors:

- health
- safety
- food
- water
- energy
- transport
- finance
- manufacturing
- information and communications technology (ICT)
- academia
- innovation
- federal government
- provincial / territorial / municipal government
- democratic institutions
- small and medium organizations
- Canadian citizens

This is crucial, because, as we stated in our 2020 National Cyber Threat Assessment, Canada's critical infrastructure will almost certainly continue to be a target for both criminal and state-sponsored cyber threat activity.

Much of the data we share is generated by HBS (see above) based on the threats that are hitting Government of Canada systems. A future goal is to tailor a version of HBS that can be deployed to key strategic partners to protect the critical infrastructure Canadians rely on.

Responding to incidents

CSE's Cyber Centre is the federal government's operational lead during cyber security events such as the SolarWinds and Microsoft Exchange compromises, as well as thousands of other cases that never make the headlines. Our teams work 24/7 to identify compromises and alert potential victims within the federal government and Canadian critical infrastructure. In the wake of a cyber incident the incident response team offers advice and support to contain the threat and mitigate harm.

In 2020-2021 the Cyber Centre responded to **2206** cyber security incident cases affecting the Government of Canada or critical infrastructure partners. That's an average of 6 per day.

Disrupting foreign threats

In 2019, the CSE Act granted CSE new powers to conduct foreign cyber operations (both active, and defensive): in other words, to take online action to disrupt foreign threats to Canada.

Over the past year, CSE has been authorized to carry out operations to interfere with foreign-based adversaries in cyberspace. These online operations have helped to defend Canada's interests and to keep Canadians safe. They are also intended to deter threat actors by changing the cost-benefit calculus of targeting Canada in future.

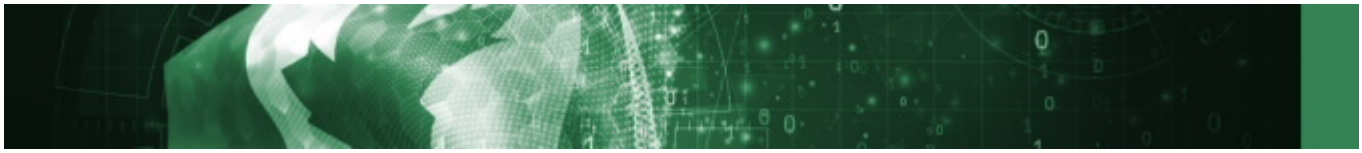
Canada's use of cyber operations follows Canadian law as well as norms of responsible state behaviour in cyberspace. For example, under the *CSE Act*, cyber operations must **not:**

- target Canadians or anyone in Canada
- interfere with the course of justice
- interfere with the course of democracy

- cause death or bodily harm, either deliberately or through criminal negligence

All our activities, including cyber operations, are subject to strict internal oversight and independent external review by the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians.

A secure digital Canada



Part of our CSE 2025 strategy is to improve Canada's overall digital resilience by fostering a national culture of cyber security.

Protecting Canada's Internet

CSE's role defending Government of Canada networks, combined with our foreign signals intelligence mandate, give us a unique perspective on the global cyber threat landscape. We offer the benefits of that perspective to all Canadians through our partnership with the Canadian Internet Registration Authority (CIRA), the not-for-profit agency that manages the .ca domain.

CIRA Canadian Shield launched officially in April 2020. It is a free, protected DNS (Domain Name System) service that prevents users from connecting to websites that have been flagged as malicious. Instead of allowing malware to infect your device, or steal your personal information, that “one wrong click” doesn’t connect. In December 2020, CIRA Canadian Shield reached its first-year goal of 100,000 users, 4 months ahead of schedule. In that period, it blocked more than 20 million malicious domains for its users.

Public reporting

CSE fosters a secure digital Canada by sharing the right information with the right audience at the right time.

For example, over the past year, the Cyber Centre published four cyber threat bulletins:

- Impact of COVID-19 on Cyber Threat Activity
- Impact of COVID-19 on Cyber Threats to the Health Sector
- Modern Ransomware and Its evolution

- The Cyber Threat to Canada's Electricity Sector

▶ Long description - Cyber Centre public reports by the numbers:

In November 2020, the Cyber Centre published its second National Cyber Threat Assessment, laying out the latest trends in the cyber threat environment from ransomware and commercial espionage to foreign influence campaigns.

A sampling of Cyber Centre guidance documents this year includes cyber security advice for individuals and organizations on topics including:

- cloud computing
- remote working
- COVID-19 and malicious websites
- online banking
- online shopping

- video-conferencing

In addition, the Cyber Centre published hundreds of advisories and alerts for IT professionals, from run-of-the-mill security patches to major cyber incidents like the SolarWinds Orion Platform and Microsoft Exchange Server compromises.

Promoting cyber resilience

The goal of a secure digital Canada means fostering the cyber resilience of every Canadian.

Get Cyber Safe

The Get Cyber Safe (GCS) public awareness campaign specializes in easy-to-follow cyber security advice presented in an informal and creative way.

Throughout the pandemic, GCS has provided Canadians with resources on topics such as COVID-19 scams, remote working and e-commerce. This included a dedicated COVID-19 resource page, share-worthy videos, timely blog posts and vibrant one-pagers.

In September 2020, CSE launched the new the Get Cyber Safe website including the GCS Checkup cyber security self-assessment tool.

In October, GCS was the Government of Canada lead for Cyber Security Awareness Month (CSAM), with the overall theme of Device Appreciation Time. The Twitter posts releasing the catchy theme song video were seen over 147,000 times.

In March 2021, GCS launched CSE's largest advertising campaign ever with the tagline *Don't Get Reeled In*. It focused on phishing, which the Cyber Centre has identified as the biggest cyber threat to Canadians, and was seen more than 74 million times.

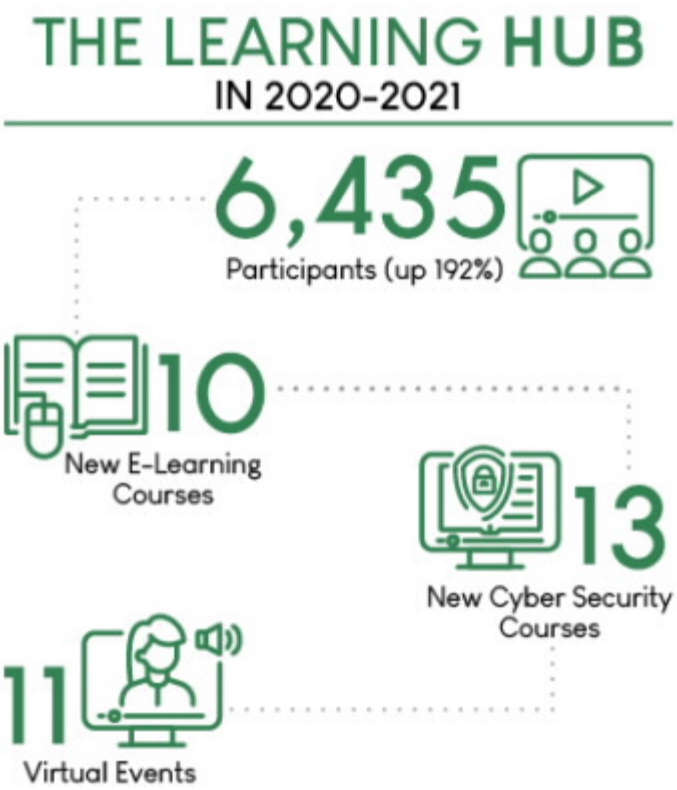
▶ Long description - GCS on social media:

Learning Hub

The Cyber Centre's Learning Hub provides training in cyber security and communications security to federal employees, and other key sectors affecting Canadians, such as industry, academia and education.

Over the past year, the Learning Hub pivoted much of its curriculum to an e-learning model, and developed and delivered new cyber security courses for groups at higher risk from cyber threats during the pandemic, including:

- healthcare workers
- researchers and academics
- federal public servants working from home
- teachers (to share with students grades 4 – 12)



▶ Long description - The Learning Hub in 2020-2021:

A Canadian information advantage

CSE promotes Canada's security and prosperity by gathering signals intelligence from foreign networks and by protecting Canada's sensitive communications.

Providing foreign intelligence insights to Canadian decision-makers

CSE's foreign signals intelligence (SIGINT) program provides Canada's senior decision-makers with insights into the activities, motivations, capabilities and intentions of foreign adversaries.

Our classified reports alert and inform government officials about threats to Canada and provide advice and guidance on practical measures to defend against them.

Over the past year, in addition to informing the government's pandemic response, CSE SIGINT has helped thwart or respond to foreign-based threats including espionage, terrorism, ideologically motivated violent extremism (IMVE), and kidnappings of Canadians abroad. Our intelligence reporting has also identified hostile state activities, supported Canadian military operations and protected forces deployed abroad.

CSE's relationships with its Five Eyes cryptologic partners (US, UK, Australia and New Zealand) bring great benefit to Canada through access to unparalleled foreign intelligence reporting on issues of common concern. On the strength of this 75-year partnership, CSE is able to provide the Government of Canada with the most comprehensive information available relating to Canada's intelligence priorities, directly furthering's Canadian safety, security and prosperity.

▶ Long description - CSE foreign intelligence reporting 2020-2021:

Providing insights into cyber threats

CSE SIGINT feeds into unclassified public reports, like the 2020 National Cyber Threat Assessment (NCTA 2020), which outlines various foreign-based cyber threats to Canada, including commercial espionage and the disruption of critical infrastructure. SIGINT supports the activities of the Cyber Centre by providing early warning to thwart and mitigate such threats.

SIGINT analysis also underpins our public attributions of malicious cyber activity. For example, in July 2020, CSE and its UK and US allies named a group of sophisticated threat actors, almost certainly operating as part of Russia's intelligence services, as the source of cyber threat activity targeting COVID-19 vaccine research.

Monitoring foreign threats to our democratic process

As noted in NCTA 2020, online interference campaigns are no longer restricted to election periods. They have become the "new normal" as adversaries use social media to:

- spread disinformation
- polarize public opinion
- discredit politicians
- influence policy decisions
- destabilize relations between countries
- delegitimize democracy

Over the past year, CSE SIGINT continued to inform the Security and Intelligence Threats to Elections (SITE) Task Force, an interdepartmental body established in 2019 to build awareness of foreign threats to Canada's electoral process and to help the Government assess and respond to those threats.

> Reminder: The *CSE Act* requires that our activities do not target the communications of Canadians or anyone in Canada. The *CSE Act* also requires that we protect the privacy of Canadians and persons in Canada. Internal audit, external oversight and independent review bodies exist to make sure we comply with the CSE Act and all other Canadian laws.

Protecting Canada's sensitive communications

The flip side of the "strategic information advantage" coin is protecting Canada's sensitive communications from our adversaries.

CSE does this by developing, approving and overseeing communications security (COMSEC) solutions for the Government of Canada. These are devices and procedures that allow authorized individuals to call, text, email and store data securely.

Despite the pandemic, the Cyber Centre continued to deliver a full suite of COMSEC services to its client departments. This year, in support of the Privy Council Office, CSE worked with Shared Services Canada to add video-calling capability for senior officials (see *Protecting the government response*). Clients include Cabinet ministers, senior government officials and decision-makers across government.

CSE also continued to operate Canada's Top Secret Network (CTSN), which allows government departments and authorized contractors to store and communicate sensitive information securely.

Thought-leading innovation

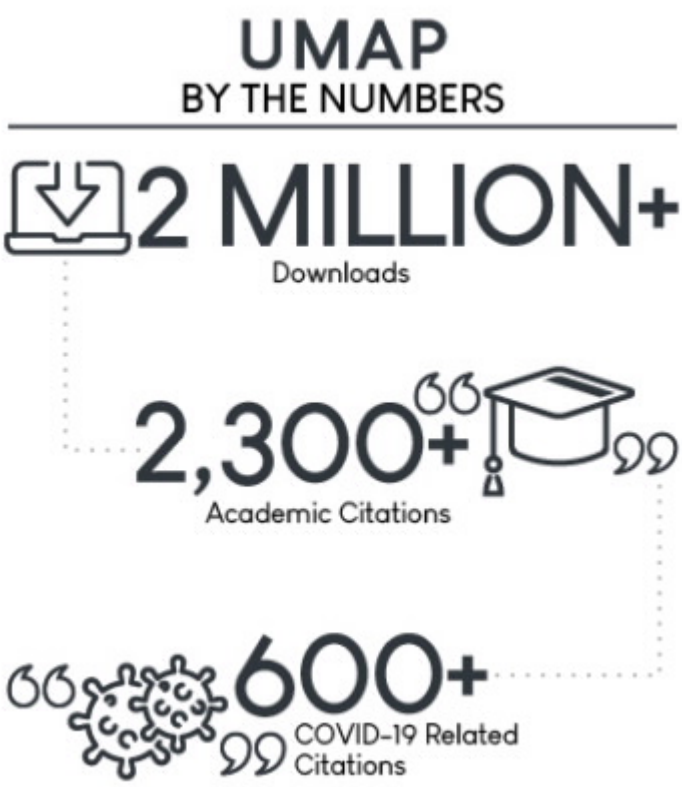
CSE cultivates an innovation mindset because the threat landscape is constantly evolving. In cyber security, you innovate, or you lose.

Innovation through research

The Tutte Institute for Mathematics and Computing (TIMC) is a government research institute within CSE, focused on fundamental mathematics and computer science. One example of the leading-edge innovation that goes on there is UMAP (Uniform Manifold Approximation and Projection).

UMAP was originally developed by Tutte Institute researchers as a technique for analyzing malware. But since they released it open-source in 2018, UMAP has been referenced in over 2300 studies ranging from machine learning to astrophysics.

In 2020 epidemiologists began to harness UMAP to analyze the vast quantities of complex data generated by the COVID-19 pandemic. To date, it has been cited in more than 600 studies related to COVID-19, from the analysis of virus variants to the search for treatment candidates.



▶ Long description - UMAP by the numbers:

Innovation through collaboration

GeekWeek is a good example of CSE's collaborative approach to innovation. It is a 9-day workshop, hosted by the Cyber Centre, where cyber security practitioners from government, industry, and academia work together to

find new solutions to shared problems.

This year, due to pandemic restrictions, GeekWeek was held in a virtual format for the first time.

Teams made breakthroughs in topics including:

- identifying and analyzing malicious phishing URLs
- studying how threat actors use virtual currency
- improving the security of:
  - emerging cloud technologies
  - Internet-connected devices
  - mobile communications

Throughout the year, the Cyber Centre and the GeekWeek community continued to collaborate on these and other projects to help build Canada's future cyber resilience.

▶ Long description - GeekWeek 2020 by the numbers:

Scanning the horizon

Recognizing CSE as a hub of innovative thinking about the future of cyber security, the National Research Council (NRC) invited CSE's Chief Research Officer to participate in a Horizon Scanning Working Group, which began work in September 2020. The NRC's goal was to identify key challenges and opportunities facing Canada in the next 10 to 15 years. The working group identified several priorities at the intersection of cyber security and privacy in Canada, including:

- hardening the cyber-resilience of digital infrastructure
- safeguarding the privacy and security of data in the cloud
- promoting Canada as a trusted storage and transit hub for international data

The NRC is due to publish its Horizon Scanning report later this year.

Addressing the quantum threat

The standard techniques used to encrypt data today will no longer be effective with the advent of quantum computing. Technology capable of breaking the cryptography we use today could be available as early as the 2030s, so CSE's Cyber Centre is preparing Canada for the future, now.

Over the past year, we shared briefings and publications with government and industry clients at both the executive and technical levels including:

- Addressing the Quantum Computing Threat to Cryptography
- Preparing Your Organization for the Quantum Threat to Cryptography
- Blog on post-quantum cryptography standards

We also worked with industry and standards organizations to advance cutting-edge quantum-safe research and worked with Government of Canada Departments to upgrade their equipment. Together these initiatives will help to ensure Canada remains a leader in quantum-safe cyber security.

Inspired workforce

Having an inspired workforce is at the centre of the CSE 2025 strategy. It is what enables us to deliver all the other aspects. We are proud to report that CSE was recognized as a Top Employer in both 2020 and 2021.

Putting people first

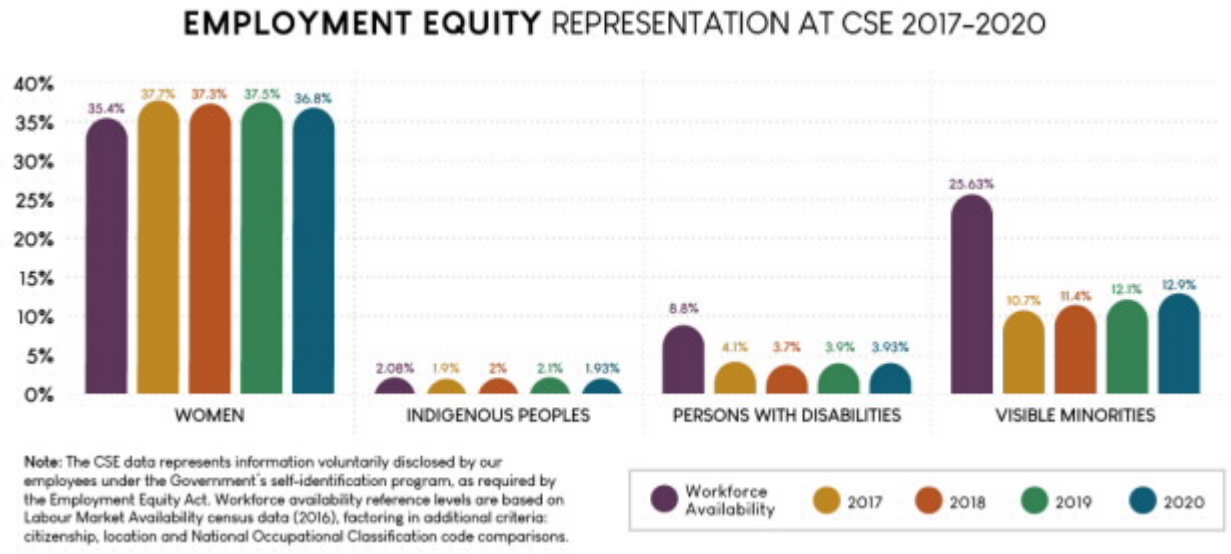
CSE's most important asset is our people.

In March 2021, CSE added a People Committee to our governance structure to make sure employees continue to come first in CSE's corporate decision-making. Chaired by CSE Chief Shelly Bruce, the committee's duties include ensuring that CSE:

- promotes workplace health and mental health
- respects Official Languages law and encourages linguistic duality
- promotes workplace accessibility
- identifies and removes systemic barriers to participation
- eliminates harassment and discrimination
- institutionalizes diversity and inclusion in our corporate processes and practices
- promotes the use of Gender-based Analysis Plus (GBA+) to inform policy and operations

Diversity and inclusion

With the exception of women, members of the federally designated Employment Equity groups are still underrepresented at CSE.



▶ Long description - Employment Equity Representation at CSE 2017-2020

One of the key tasks of CSE's new People Committee is to ensure that CSE examines its corporate policies through the lens of equity, diversity and inclusion. This includes recruitment and retention policies, as well as awareness training, program design and implementation.

The Committee is supported by an advisory group of employees from diverse backgrounds to ensure that underrepresented groups have a say in the decision-making. The advisory group will work with key human resources leaders to translate those perspectives into principle-based policy and tangible outcomes.

New training

This year, CSE worked to address systemic barriers for transgender and non-binary persons by providing training to colleagues involved in recruitment. We also began looking at other policies and practices to

remove any discriminatory practices based on gender identity or gender expression.

In February 2021, two CSE employees delivered an online presentation titled “Being Black in Canada” to hundreds of their co-workers and executives. The presenters shared powerful examples of discrimination from their own lives, led a discussion on privilege and shared anti-racism resources. CSE is building a version of the presentation into our mandatory training for new employees.

Celebrations

Our in-person

celebrations of diversity had to be adapted or put on hold this year. For instance, CSE’s LGBTQ2+ community, allies and executives usually march in Ottawa’s Pride parade. Instead, CSE decorated our facilities in rainbow colours and celebrated Pride Week on social media.

Crucial conversations

In January 2021, international speaker and psychologist, John Amaechi OBE, led a CSE-wide event discussing racism, discrimination and the importance of cultivating a respectful and inclusive workplace culture.

In March 2021, CSE hosted a virtual panel discussion where six employees spoke frankly about the disproportionate impact of COVID-19 along gender lines.

That same month, CSE employees invited an Indigenous leader with a background in signals intelligence to build cultural understanding and discuss ways CSE can promote reconciliation.

Throughout the pandemic, CSE's Diversity and Inclusion online discussion channel has provided a safe space for sharing personal experiences and exchanging resources on how to be an effective ally for marginalized communities. The channel has more than 900 members (over a quarter of the organization).

These important conversations have already begun to enhance CSE's workplace culture. We are committed to translating them into more concrete actions this year.

Employee wellbeing

Recognizing the impact of the pandemic on mental health, CSE held training courses and speaker events on topics such as self-compassion, managing anxiety and parenting in the pandemic.

Our internal communications team sent out regular reminders about the supports available to employees.

CSE's Counselling and Advisory Program shifted its services online including:

- training courses

- individual counselling
- conflict management services
- support for distributed teams (new)
- weekly guided meditations in French and English (new)

The pivot to remote work

Before the pandemic, most CSE staff based at our secure headquarters could not even access unclassified work emails from outside the building, so pivoting to remote work was no easy task.

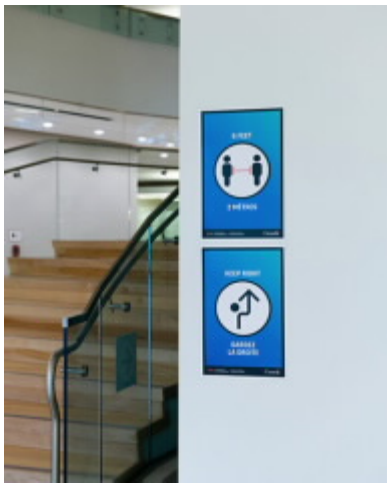
The Cyber Centre was already working in a secure cloud environment, and CSE had a long-term plan to enable similar capabilities for the rest of the agency. When the pandemic hit, that long-term plan turned into an urgent requirement overnight.

In the space of two weeks in March 2020, CSE teams:

- deployed secure mobile devices to employees
- migrated workloads to a secure cloud environment
- enabled new capabilities to allow employees to work and communicate from remote locations

Thanks to these extraordinary efforts, CSE has been able to maintain its daily operations and deliver important results for Canada throughout the past year, despite many of our employees working primarily from home.

Staying safe on site



Our classified work can only be done “on the high side”, so we took steps to make working at our facilities as safe as it can possibly be. This included:

- reconfiguring workspaces and common areas
- staggering work schedules
- mandating mask use
- reinforcing public health guidelines including staying home when sick

Our cleaning team deserves special recognition for maintaining enhanced standards throughout the year.

We had no recorded cases of COVID-19 transmission in our workplaces during the reporting period.

Employee survey results

The 2020 Public Service Employee Survey included new questions about mental health, racism, and working during the pandemic. CSE’s PSES results highlighted that:

- 91% of employees feel CSE has clearly communicated the mental health services and resources that are available to them
- 87% would feel free to speak out about racism in the workplace without fear of reprisal
- 84% are satisfied with the measures CSE has taken to protect their physical health and safety during the pandemic

While these numbers are above the public service average (84%; 79% and 81% respectively), there is still room for improvement.

Understandably, the percentage of employees who said they were experiencing work-related stress increased during the pandemic (9% in 2019; 15% in 2020).

▶ Long description - Selected statistics from CSE's Public Service Employee Survey results

Based on this feedback, CSE has identified three areas of focus for 2021:

- Managing work-life balance, stress and mental health
- Holding conversations and taking actions that promote equity, diversity and inclusion
- Helping management and employees adapt to shifting "future of work" realities

CSE will keep working to ensure our employees have what they need to deliver their mission for Canada and Canadians.

Outreach

Pandemic restrictions forced us to put some of our community outreach activities on hold this year, such as our coding workshops in local elementary schools. But CSE volunteers found ways to share their skills with the next generation of tech talent, virtually.

From November 2020 to March 2021, CSE volunteers delivered nine cyber security presentations, reaching roughly 220 high school students across the National Capital Region.

We continued our partnership with **Hackergal**, a Canadian not-for-profit that introduces girls, trans girls and non-binary students to coding. This year CSE volunteers:

- mentored students
- judged hackathon submissions
- sat on virtual panels
- gave speeches
- wrote blogs
- created learning videos
- contributed content for Black History Month
- ran a social media takeover

We continued our partnership with **Cyber Titan**, and provided content for their online cyber defence competition for Canadian youth in grades 7 - 12.

In July 2020 CSE volunteers began working with **Black Boys Code**, an organization that inspires young Black men to become tomorrow's digital creators and technological innovators.

Known and trusted

Because much of CSE's work is classified, it is vital that we have robust systems of oversight and accountability, so Canadians can be confident that CSE respects the law and protects their privacy.

The *CSE Act*, which came into force in August 2019, created three new bodies to strengthen the independent, external oversight of CSE's activities:

- The Office of the Intelligence Commissioner (ICO)
- The National Security and Intelligence Review Agency (NSIRA)
- The National Security and Intelligence Committee of Parliamentarians (NSICOP)

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

Intelligence Commissioner

The Office of the Intelligence Commissioner provides quasi-judicial oversight of CSE's foreign intelligence and cyber security ministerial authorizations before they can come into effect.

On January 27, 2021, the Intelligence Commissioner, the Honourable Jean-Pierre Plouffe, tabled his first annual report (2019).

In it, the Commissioner reviewed CSE's five ministerial authorizations from July 2019 (when the Commissioner's office was created) to the end of the calendar year. In all five cases, the Commissioner found that the conclusions on the basis of which the Minister of National Defence issued the authorizations were reasonable and valid.

The Commissioner also made several recommendations for improvement, which CSE accepted and implemented.

The Commissioner noted this improvement in his 2020 annual report, which was tabled in Parliament on April 30, 2021.

In it, the Commissioner acknowledged that CSE "displayed a continuous commitment to improving their processes and submissions, despite the challenges and the burden of the pandemic." (p. 3)

> "Although this new oversight framework was only in its second year, I am encouraged by the positive developments of this past year."
>
> - Hon. Jean-Pierre Plouffe, Intelligence Commissioner, Annual Report 2020

The report reviewed CSE's four ministerial authorizations for the 2020 calendar year and found all four to be reasonable and valid.

The Commissioner made further suggestions to improve the clarity and completeness of the application records. However, he also noted that "these issues were not detrimental to the reasonableness of the Minister's

conclusions or the [Intelligence Commissioner's] approval of these authorizations" (p. 17). CSE welcomes the Intelligence Commissioner's perspective on how to improve on the Ministerial Authorization process.

National Security and Intelligence Review Agency (NSIRA)

The National Security and Intelligence Review Agency is an independent review agency whose mandate is to scrutinize all national security and intelligence activities across the federal government.

On December 11, 2020 NSIRA's first annual report was tabled in Parliament.

In relation to CSE, the report noted that:

- CSE has developed and rolled out comprehensive policy suites to guide information sharing with foreign partners (p. 45)
- CSE employed privacy compliance measures in a timely manner and according to policy (p. 65)
- CSE complied with the law in relation to a particular privacy incident concerning metadata analysis (p. 77)

On March 4, 2021 NSIRA released its first review of CSE's self-identified privacy incidents. It made five recommendations, all of which CSE accepted.

National Security and Intelligence Committee of Parliamentarians (NSICOP)

The National Security and Intelligence Committee of Parliamentarians is made up of members of the House of Commons and the Senate who have full security clearance. It has a broad mandate to review Canada's national security and intelligence organizations, including CSE.

NSICOP's 2020 annual report was tabled in Parliament on April 12, 2021. Approximately one fifth of the report was devoted to malicious cyber activities, which NSICOP characterized as "a serious and growing risk to

Canada's national security" (p. 46).

The report was focused on updating the threat assessment first undertaken by the Committee in 2018. It was not a review, therefore there were no findings or recommendations related to CSE's activities. However, the conclusion did recognize "the efforts of the security and intelligence organizations to provide documentation in response to Committee requests despite grappling with their own pandemic-related challenges" (p. 43).

CSE will continue to support all our oversight bodies by providing the information they need to review CSE's activities on behalf of Canadians.

Quick facts

Year-at-a-glance

- April 2020: Cyber Centre helps House of Commons set up virtual Parliament
- May: Cyber Centre issues advice for COVID-19 research organizations
- June: Cyber Centre publishes second 2020 bulletin on threats to the health sector
- July: CSE and allies name Russia-linked group behind targeting of vaccine research
- September: Get Cyber Safe launches new website
- October: First ever virtual GeekWeek

- November: Cyber Centre publishes 2020 National Cyber Threat Assessment
- December: CIRA Canadian Shield reaches 100,000 users
- January: Cyber Centre begins work to secure COVID-19 vaccine rollout
- February: First Cabinet meeting with secure video-conferencing
- March: CSE and partners reach 7000 takedowns of fraudulent COVID-19 websites

CSE-at-a-glance

- CSE was formally established in 1946 as the Communications Branch, National Research Council.
- In 1975, it was renamed the Communications Security Establishment and moved to the National Defence portfolio.
- In November 2011, CSE became a stand-alone agency, reporting to the Minister of National Defence.
- The current Chief of CSE, Shelly Bruce, was appointed in June 2018.
- The Canadian Centre for Cyber Security launched in October 2018 uniting expertise from across the federal government under one roof. It is part of CSE.
- CSE's governing legislation, the *CSE Act* came into force in August 2019.
- CSE's 2020-2021 budget is $794 million. *
- Our workforce is just under 3000 strong. **

- On September 1, 2021, CSE will celebrate its 75th anniversary.

Footnotes

[*] Total authorities

[**] 2992 full-time employees as of March 31, 2021. Does not include part-time employees, contractors or students.

Date modified:
2021-06-28