National Cyber Security Action Plan

2019-2024

Budget 2018 Investments

Public Safety Canada
Sécurité publique Canada

Canada

Cat. No.: PS9-1/2019E-PDF
ISBN: 978-0-660-31467-9

TABLE OF CONTENTS

Minister's Message 1

Introduction 2

Goal 1 Secure and Resilient Systems 4

- Supporting Canadian Critical Infrastructure Owners and Operators
- Improved Integrated Threat Assessments
- Preparing Government of Canada Communications for Advances in Quantum
- Expanding Advice and Guidance to the Finance and Energy Sectors
- Cyber Intelligence Collection and Cyber Threat Assessments
- National Cybercrime Coordination Unit
- Federal Policing Cybercrime Enforcement Capacity

Goal 2 An Innovative and Adaptive Cyber Ecosystem 10

- Cyber Security Component of the Student Work Placement Program
- Cyber Security Assessment and Certification for Small and Medium-Sized Enterprises (SMEs)

Goal 3 Effective Leadership, Governance and Collaboration 14

- Strategic Policy Capacity in Cyber Security and Cybercrime
- Cyber Security Cooperation Program
- Canadian Centre for Cyber Security
- International Strategic Framework for Cyberspace
- Bilateral Collaboration on Cyber Security and Energy

Conclusion 20

MINISTER'S MESSAGE

The Honourable Ralph Goodale
Minister of Public Safety and Emergency Preparedness

Every day, Canadians are online – more so than people anywhere else in the world – for work, play, shopping, banking, business, getting our news and just staying in touch. Yet the same digital infrastructure that so enhances our quality of life can also leave us vulnerable to those who would do us harm. From the critical infrastructure underpinning our Canadian economy, to commercial supply chains, to social networks and personal conveniences, the cyber threats to Canadian systems are large and growing, putting Canadians at risk. Cybercrime in Canada causes more than $3 billion in economic losses each year.

To better address this huge contemporary challenge, the Government of Canada conducted a comprehensive Cyber Review, beginning in 2016, which included the first-ever public consultations on the topic, augmenting the insights gained from many experts and key stakeholders in both the private and public sectors.

That review led to Canada's new National Cyber Security Strategy, released in 2018, with initial funding in the 2018 and 2019 federal budgets totalling close to $1 billion. The strategy is designed to be adaptable, taking into account the continuously changing cyber landscape. It also recognizes that the demand for bright new cyber security solutions will create excellent jobs and drive economic growth. Budget 2019 included $145 million to help to protect Canada's critical cyber systems including in the finance, telecommunications, energy and transport sectors. Budget 2019 also included $80 million over four years to support three or more Canadian cyber security networks across Canada that are affiliated with post-secondary institutions. The networks—to be selected through a competitive process—will expand research, development and commercialization partnerships between academia and the private sector.

The strategy has three prime goals – secure and resilient Canadian information technology systems in government and beyond; a fertile cyber environment for Canadian science, innovation, talent and entrepreneurship; and strong domestic collaboration across our country, leading to Canadian leadership in shaping international developments with respect to cyber security.

This document takes the next step. In this National Cyber Security Action Plan (2019-2024), we lay out the specific initiatives planned over the coming five years to bring the strategy to life. In government, the private sector and our personal use, the plan is intended to empower Canadians to improve their cyber security and market their cyber skills and innovations to the world – generating well-paid middle-class jobs and a more prosperous Canada.

INTRODUCTION

As a global society, we have gone digital. We play, learn, socialize, communicate and do business online. While the digital economy brings significant benefits, it also exposes significant vulnerabilities that can be exploited.

In 2010, the Government of Canada (the Government) launched a national effort to defend against cyber threats with Canada's first Cyber Security Strategy. As the digital economy evolves, so do cyber threats, requiring a refreshed strategy that responds to the changing landscape. In 2016, we took the first step toward developing a new Cyber Security Strategy. A comprehensive Cyber Review was launched and included Canada's first public consultation on cyber security, gaining insights and advice from experts, key stakeholders, and engaged citizens.

The new National Cyber Security Strategy (the Strategy), released in 2018, responds to the Cyber Review. It recognizes that robust cyber security is an essential element of Canadian innovation and prosperity. The Strategy is designed to be adaptable and to account for a continuously changing cyber landscape.

The Strategy introduces this new strategic direction and defines three goals to achieve its vision of *security and prosperity in the digital age*:

- **Secure and Resilient Canadian Systems:** with enhanced capabilities and in collaboration with partners, the Government of Canada will better protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems.
- **An Innovative and Adaptive Cyber Ecosystem:** The Government of Canada will support advanced research, foster digital innovation, and develop cyber skills and knowledge to position Canada as a global leader in cyber security.
- **Effective Leadership, Governance and Collaboration:** In collaboration with provinces, territories, and the private sector, the federal government will take a leadership role to advance cyber security in Canada, and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.

This document, the *National Cyber Security Action Plan (2019-2024)* for Canada's new Cyber Security Strategy, is a blueprint for the implementation of the Strategy. It sets out the initiatives and milestones supporting each of our three goals, and presents a roadmap of how we will achieve and maintain our vision of security and prosperity in the digital age. Funded through Budget 2018 ($507.7M over 5 years, and 108.8M ongoing), these initiatives represent an incremental first step to achieving this vision. As the Strategy is designed to be flexible, it is anticipated that additional initiatives could be identified as the cyber landscape continues to evolve.

Goal 1

Secure and Resilient Systems

Through collaborative action with partners and enhanced cyber security capabilities, we will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems.

As malicious cyber tools become increasingly accessible, and as rates of cybercrime continue to rise, there is a real threat to Canada's economic well-being. As more of Canada's critical infrastructure can be controlled remotely and essential services are managed online, cyber incidents have the potential to compromise national security and public safety. To address these risks, the Government of Canada will expand its efforts to support Critical Infrastructure (CI) owners and operators in reducing their cyber security risks. It will do so by providing CI owners and operators with enhanced awareness of cyber risks and vulnerabilities, and of the mitigation measures available to enhance the resilience of vital infrastructure systems. The Government of Canada will also enhance law enforcement capacity

to respond to cybercrime by supporting coordination across law enforcement agencies and with federal, provincial, territorial, and international partners. The Government will enhance cybercrime investigative capacity and make it easier for Canadians to report cybercrime.

INITIATIVES

Supporting Canadian Critical Infrastructure Owners and Operators

The Department of Public Safety and Emergency Preparedness will deliver a comprehensive risk management approach that will enable CI owners and operators to better secure their systems and information. Specifically, the Department will increase its capacity to: 1) conduct cyber security assessments to help organizations identify and address vulnerabilities in their cyber systems, including through the use of a technical network assessment tool; 2) provide sector stakeholders with information on the latest threats and trends affecting industrial control system (ICS) security, and offer hands-on technical training to mitigate risks and strengthen ICS resilience, including through the delivery of ICS Security Symposiums; and 3) coordinate and deliver cyber-based exercises for the CI community to help test and develop individual/collective capabilities to respond to, and recover from, cyber-attacks.

Improved Integrated Threat Assessments

The new Canadian Centre for Cyber Security (the Cyber Centre), housed within the Communications Security Establishment (CSE), will increase its capacity to produce all-source strategic cyber threat assessments and contextualize cyber threats to assist the Government of Canada and Canadians in understanding complex and evolving cyber threats (e.g. 2019 Update: Cyber Threats to Canada's Democratic Process). A better understanding of the cyber threat landscape by the Government of Canada and Canadians will facilitate better responses and a more cyber secure and resilient Canada.

Preparing Government of Canada Communications for Advances in Quantum

In order to protect the confidentiality of today's Government of Canada communications against future attacks by quantum computing, CSE will undertake the Interim Quantum Safe Capability project in collaboration with other Government departments to ensure the Government of Canada's classified cryptographic devices are appropriately updated.

Expanding Advice and Guidance to the Finance and Energy Sectors

The Cyber Centre will enhance its partnerships with owners and operators of critical infrastructure in the Canadian finance and energy sectors thereby enabling the mutually beneficial exchange and co-

development of unique cyber security knowledge and capabilities in order to better defend against advanced cyber threats.

Cyber Intelligence Collection and Cyber Threat Assessments

With enhanced funding in support of the Strategy, the Canadian Security Intelligence Service (CSIS) will increase the work already being done in cyber intelligence collection and cyber threat assessments. It will support analysis to better understand cyber threats and the intentions and capabilities of cyber actors operating in Canada and abroad who pose a threat to the security of Canada. This will enable the Government of Canada to improve its overall situational awareness, better identify cyber vulnerabilities, mitigate or prevent cyber espionage, sabotage, foreign interference, or other cyber threat activity, and take action to secure critical infrastructure.

National Cybercrime Coordination Unit

The Royal Canadian Mounted Police (RCMP) will establish the National Cybercrime Coordination Unit (NC3 Unit) to coordinate Canadian police operations against cybercriminals and to establish a national mechanism for Canadians and businesses to report cybercrimes to police.

The NC3 Unit will:

- Coordinate Canadian cybercrime operations and collaborate with international partners;
- Provide digital investigative advice and guidance to Canadian police;
- Produce actionable cybercrime intelligence for Canadian police;
- Collaborate with CSE's Canadian Centre for Cyber Security; and,
- Establish a national public reporting mechanism for Canadians and businesses to report cybercrimes and fraud to law enforcement.

> *"The threats we face in cyberspace are complex and rapidly evolving. Governments, businesses, organizations, and Canadians are vulnerable. With more of our economy and essential services moving online every year, the stakes could not be higher. (The Strategy)"*

Federal Policing Cybercrime Enforcement Capacity

The RCMP will also enhance its operational capacity (investigations, intelligence, specialized technical investigative services, international presence, and specialized cyber expertise) to take federal enforcement action against priority cybercrime activity both domestically and internationally. More specifically, the RCMP will:

- Enhance capacity to target cybercrime related criminal activities;
- Enhance specialized cyber capability to federal investigative teams and increase capacity to respond to and participate in joint investigations with Canada's key international law enforcement partners; and,
- Detect, prevent, and respond to threats to the safety and security of Canadians and Canadian interests.

Goal 1 Secure and Resilient Systems

Supporting Canadian Critical Infrastructure Owners and Operators

Department	Action/Milestone	End Date	Status
Public Safety Canada (PS)	Acquire/develop a technical cyber assessment tool	2019	Planned
	Establish an Industrial Control System (ICS) Advisory Committee	2019	Planned
	Increase the number of cyber security exercises delivered to critical infrastructure stakeholders	2020	Planned
	Develop technical ICS security training and awareness solution	2020	Planned

Improved Integrated Threat Assessments

Department	Action/Milestone	End Date	Status
Communications Security Establishment (CSE)	Increase capacity to enable CSE to better meet increasing demands for cyber threat assessments	2024	In Progress
	Increase capacity to enable CSE to assess a wider array of cyber threats reflecting the Cyber Centre's growing client base	2024	In Progress

Preparing Government of Canada Communications for Advances in Quantum

Department	Action/Milestone	End Date	Status
Communications Security Establishment (CSE)	Protect Government of Canada's classified information against anticipated advancements in quantum computing	2024	In Progress

Expanding Advice and Guidance to the Finance and Energy Sectors

Department	Action/Milestone	End Date	Status
Communications Security Establishment (CSE)	Finance and energy sectors work cooperatively with the Cyber Centre and within their sectors to improve their cyber security postures	2024	In Progress
	Improve cyber security posture of the finance and energy sectors	2024	In Progress

Cyber Intelligence Collection and Cyber Threat Assessments

Department	Action/Milestone	End Date	Status
Canadian Security Intelligence Service (CSIS)	Augment CSIS collection of national security cyber intelligence and cyber threat assessments	2024	Planned

National Cybercrime Coordination Unit (NC3 Unit)

Department	Action/Milestone	End Date	Status
Royal Canadian Mounted Police (RCMP)	Reach initial operating capability	2020	In Progress
	Establish NC3 Unit Advisory Group	2021	In Progress
	Launch the National Cybercrime and Fraud Public Reporting System	2022	In Progress
	Reach full operating capability	2023	In Progress

Federal Policing Cybercrime Enforcement Capacity

Department	Action/Milestone	End Date	Status
Royal Canadian Mounted Police (RCMP)	Deploy cyber specialists abroad	2020	In Progress
	Establish/support cybercrime investigative teams	2021	In Progress
	Recruit/train cyber capability specialists	2021	In Progress

Goal 2

An Innovative and Adaptive Cyber Ecosystem

By supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge, the federal government will position Canada as a global leader in cyber security.

Cyber security is increasingly driving innovation and economic activity in Canada. Governments, academia, and members of the private sector can work together to create new opportunities, drive investment, and foster leading-edge research and development. Moreover, the demand for qualified cyber security professionals represents an immediate and growing opportunity for Canada's highly educated workforce.

The Government of Canada will play a leadership role in supporting advanced research and helping innovative companies scale up to bring cyber security technologies and services to the global marketplace. It will work with partners to drive investment and foster cyber research and development. It will also invest in initiatives that support digital skills development to address the cyber skills gap, with aims of building the labour force for the future.

INITIATIVES

Cyber Security Component of the Student Work Placement Program

Led by the Department of Employment and Social Development Canada (ESDC), this initiative will be used to resource a component of the Student Work Placement (SWP) Program to support the creation of up to 1,000 new Work-Integrated Learning (WIL) opportunities over three years in cyber security.

The SWP Program currently supports the creation of WIL opportunities for Canadian students to align the skills of graduates with the hiring needs of employers in growing industries. Eligible participants must be enrolled in science, technology, engineering, mathematics (STEM) and business programs at post-secondary education institutions across Canada. WIL opportunities provide students with valuable skills development opportunities to facilitate a smoother transition from school to work upon graduation, and help employers build a talent pipeline for their future hiring needs. The SWP supports collaborative partnerships that bring together employers and willing post-secondary education institutions to work on innovative ways of aligning educational skills development with the skills requirements of employers in key and emerging sectors of the Canadian economy.

The SWP Program provides employers with wage subsidies of 50% for each new standard work placement they create (up to a maximum of $5,000 per placement). This wage subsidy is higher, 70% (up to a maximum of $7,000), for new placements created for under-represented students, including women in STEM, Indigenous peoples, Persons with Disabilities, and newcomers; as well as first-year students.

The cyber security component of the SWP will focus on increasing the number of WIL opportunities for Canadian students in cyber security to ensure talented young Canadians are graduating with the full complement of skills employers are looking for.

Cyber Security Assessment and Certification for Small and Medium-Sized Enterprises (SMEs)

Businesses in Canada, especially Small and Medium Enterprises (SMEs), do not have the same capacities as larger businesses when it comes to cyber security. The introduction of a voluntary certification for individual businesses will help participants position their competitive advantage and promote trust in the digital economy. The Cyber Certification Program is geared towards SMEs, which approximately make up 98% of the total number of businesses in Canada.

While a small number of standards for cyber security exist, the Cyber Certification Program requires the implementation of specific cyber security controls by participants certified by a third party accredited certification body to ensure a consistent application of cyber security protections to demonstrate a baseline security provided by certified businesses. This Program is designed to be a starting point for SMEs to improve their cyber security posture.

The ultimate purpose of the Cyber Certification Program is to raise the cyber security posture among Canadian SMEs, increase consumer confidence in the digital economy, promote international standardization, and better position SMEs to compete globally. This public-private initiative is led by Innovation, Science, and Economic Development Canada (ISED), in collaboration with the Communications Security Establishment (CSE), Standards Council of Canada (SCC) and independent private sector accredited certification bodies.

> *Digital innovation has become the engine of economic growth in the 21st century. Cyber security is not only essential for protecting the sources of Canada's digital innovation – it has become a source of innovation in its own right. (The Strategy)*

Goal 2 An Innovative and Adaptive Cyber Ecosystem

Cyber Security Student Work Placement Program

Department	Action/Milestone	End Date	Status
Employment and Social Development Canada (ESDC)	Launch student work-integrated learning program	2019	Completed
	Complete student work-integrated learning program and conduct evaluation	2021	Planned

Cyber Security Assessment and Certification for Small and Medium-Sized Enterprises (SMEs)

Department	Action/Milestone	End Date	Status
Innovation, Science, and Economic Development (ISED), with CSE and SCC	Develop security controls in collaboration with CSE	2019	Completed
	Launch cyber education and awareness tool	2019	In Progress
	Launch cyber certification program	2019	In Progress
	Launch national standard for cyber security	2020	Planned

Goal 3

Effective Leadership, Governance and Collaboration

The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada and will, in coordination with allies, work to shape the international cyber security environment in Canada's favour.

The Government of Canada will demonstrate leadership in advancing Canada's cyber security interests both domestically and abroad, by ensuring the enhanced collaboration and coordination of strategic cyber security and cybercrime issues amongst stakeholders, and by advocating for an open, free and secure internet. Establishing a clear focal point for cyber security within the federal government, through the newly established Canadian Centre for Cyber Security, will demonstrate leadership, while ensuring that partners receive unified advice and guidance on cyber security and

cybercrime issues. The Government of Canada will work to increase information sharing amongst domestic and international partners, and to collect relevant data and metrics in support of evidence-based decision-making.

INITIATIVES

Strategic Policy Capacity in Cyber Security and Cybercrime

With an enhanced strategic policy team responsible for cyber security and cybercrime issues, the Department of Public Safety and Emergency Preparedness will be better positioned to support the expanded range of functions to be undertaken to implement the new National Cyber Security Strategy. This initiative will help ensure the proper coordination of strategic cyber security and cybercrime policy issues amongst internal and external stakeholders, allow the Department to begin preliminary work to address the cyber security and cybercrime data gaps, and allow for the resources necessary to support the expanded Cyber Security Cooperation Program (CSCP).

By enhancing its strategic policy capacity, the Department will be better positioned to absorb research emanating from funded CSCP projects. This will help inform future-oriented work, develop proactive policy solutions to emerging issues, and help position the Government to anticipate trends and developments.

Cyber Security Cooperation Program

The Cyber Security Cooperation Program (CSCP) is the only Government of Canada grants and contributions program dedicated to supporting projects aimed at improving the security of Canada's cyber systems. While originally launched as a pilot program, Budget 2018 allocated additional funding for its renewal and expansion. The expanded CSCP will be aligned with the goals of the new National Cyber Security Strategy, allowing it to deliver more ambitious results in support of all three goals of the NCSS, with a particular focus on innovation and research.

The program will support a range of stakeholders, such as academic and research institutions, small- and medium-sized enterprises, and other private sector partners. Projects supported through the CSCP will yield comprehensive results that help position Canadian governments, businesses, and citizens to better anticipate trends, adapt to a changing environment, and remain on the leading edge of innovation in cyber security. By supporting Canadian research efforts, the CSCP will help improve the collective understanding of the cyber landscape, and advance Canada's economic position.

Canadian Centre for Cyber Security

Until recently, the Government of Canada's cyber security operational capabilities were distributed across different departments and agencies. Though measures were in place to ensure good communication and coordination, ambiguity concerning roles and responsibilities and the inherent difficulty in coordinating multiple decision makers was a barrier to the quick, effective, clear, and trusted technical guidance that Canadians have come to expect from their government. To address this gap, the Government of Canada established the new Canadian Centre for Cyber Security (the Cyber Centre) within the Communications Security Establishment (CSE) in October 2018. It is a single, unified team of government cyber security technical experts that will be the definitive source of unique technical advice, guidance, services, messaging and support on cyber security operational matters for government, critical infrastructure owners and operations, the private sector and the Canadian public. Canadians will have a clear and trusted place to turn to for all cyber security operations issues. The Centre will also provide cyber security expertise to support lead agencies in the delivery of their core functions, including collaborating with the RCMP's NC3 and its law enforcement efforts to address cybercrime.

International Strategic Framework for Cyberspace

The international dimension of cyber security has not been the focus of Canadian action to date, despite the fact that many threats originate from abroad and that cyber security is an inherently transnational issue. The United States (U.S.), Canada's largest economic and trading partner, is at the forefront of efforts to address international aspects of cyber security, and is looking to allies to cooperate closely by making a significant contribution to these international efforts. Global Affairs Canada's (GAC) International Strategic Framework for Cyberspace will allow Canada to enhance its cooperation with the U.S. as it further implements its cyber security strategy, including by putting in place personnel in Washington to facilitate closer collaboration. GAC will also establish an International Cyber Engagement Working Group to enhance information sharing and coordination between government organizations working on international cyber issues. This initiative supports GAC's mandate to enhance and promote Canada's leadership in an evolving global context, including by advancing efforts to more effectively fulfill Canada's commitments within the North Atlantic Treaty Organization (NATO) and other regional organizations, such as the Organization for Security Cooperation in Europe (OSCE), the Organization of American States (OAS), and the ASEAN Regional Forum (ARF).

Bilateral Collaboration on Cyber Security and Energy

Building on current strengths and expertise, Natural Resources Canada (NRCan) will enhance its capacity to collaborate with energy sector stakeholders (e.g., federal departments, provinces and territories, private industry, the U.S.) on cyber security and critical energy infrastructure protection. Envisioned as a collection of bilateral activities, this initiative will facilitate improved two-way communication and cooperation in the face of an increasingly pervasive and sophisticated cyber threat environment. In particular, NRCan aims to pursue joint activities with the U.S. that will strengthen the security and resiliency of the integrated North American electricity grid and cross-border pipelines. To this end, these activities will deliver on the pillars of prevention, preparedness, response and recovery by contributing to more secure and resilient energy systems, developing and strengthening the preparedness capabilities of the energy sector to cyber-attacks, and establishing joint mechanisms to bolster response and recovery of government entities and the energy sector. Ultimately, this initiative will position Canada to better address and respond to both domestic and international threats to our nation's critical energy infrastructure.

Goal 3 Effective Leadership, Governance, and Collaboration

Strategic Policy Capacity in Cyber Security and Cybercrime

Department	Action/Milestone	End Date	Status
Public Safety Canada (PS)	Recruit strategic policy team	2022	In Progress
	Undertake annual progress review	2021-2024	Planned
	Undertake governance review	2021	Planned

Cyber Security Cooperation Program (CSCP)

Department	Action/Milestone	End Date	Status
Public Safety Canada (PS)	Launch the renewed CSCP	2019	Planned
	Conduct program marketing	2019	Planned
	Initiate Call for Proposals	2019	Planned
	Disburse project funding	2019	Planned

Canadian Centre for Cyber Security

Department	Action/Milestone	End Date	Status
Communications Security Establishment (CSE)	Virtual launch of the Canadian Centre for Cyber Security (the Cyber Centre)	2018	Completed
	Achieve basic operating capability	2022	In Progress
	Achieve full operating capability	2023	In Progress

Goal 3 Effective Leadership, Governance, and Collaboration

International Strategic Framework for Cyberspace

Department	Action/Milestone	End Date	Status
Global Affairs Canada (GAC)	Launch International Cyber Engagement Working Group	2018	Completed
	Create cyber unit at Global Affairs Canada	2019	Completed
	Develop International Cyber Strategy	2019	In Progress
	Undertake cyber-related capacity building	2019	In Progress
	Develop attribution policy	2019	Completed
	Staff Washington Mission position	2020	In Progress
	Host relevant cyber security meetings	2024	In Progress
	Support international participants in cyber negotiations	2024	In Progress
	Promote Canadian interests and values on cyber issues in international forums	2024	In Progress

Bilateral Collaboration on Cyber Security and Energy

Department	Action/Milestone	End Date	Status
Natural Resources Canada (NRCan)	Recruit and hire core staff for the Bilateral Collaboration Team	2019	In Progress
	Launch initial call for expressions of interest and proposals for projects	2019	Completed
	Sign contribution agreements and disburse funding for first round projects	2019	In Progress
	Launch second call for expressions of interest and proposals for projects (if required)	2020	Planned
	Sign contribution agreements and disburse funding for second round projects (if required)	2020	Planned
	Participate in key information sharing activities, workshops, and briefing sessions with the U.S. government	2023	In Progress
	Advance joint initiatives with U.S. partners on cyber security and energy (e.g. tabletop exercises, R&D, information sharing)	2023	In Progress

CONCLUSION

This Action Plan presents the blueprint for the implementation of the Strategy. Cyber security is a shared responsibility, and we are committed to working closely with other levels of government, the private sector, international partners and Canadian citizens to adapt to the changing cyber landscape. Working together, we will build a secure and prosperous Canada in the digital age.