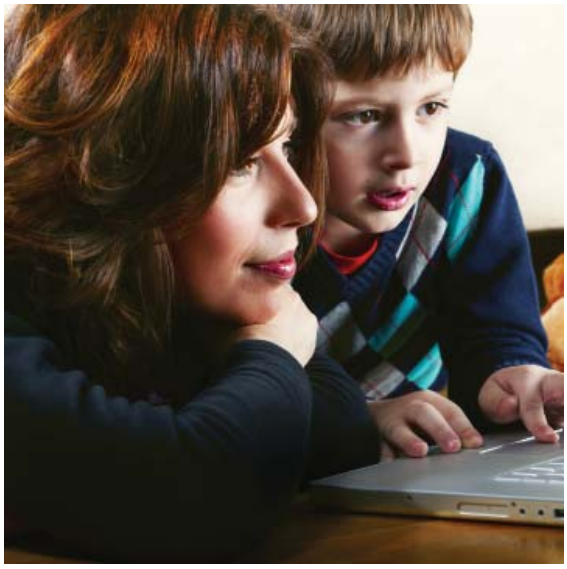
Government of Canada | Gouvernement du Canada



Action Plan 2010-2015
for Canada's Cyber Security Strategy

Canada

Cat: PS9-1/2013E-PDF
ISBN: 978-1-100-21895-3

Introduction

Information technology is highly integrated into our everyday lives. As a society, we have gone digital. We play, learn, socialize, communicate, and do business online. While cyberspace brings significant benefits, our ever increasing reliance on it is creating new and significant vulnerabilities.

In line with the Government of Canada's (the Government) commitment to keep the nation safe, secure, and prosperous, we launched *Canada's Cyber Security Strategy* (the Strategy) on October 3, 2010. The Strategy is designed to guide the Government's efforts to make cyberspace more secure for all Canadians.

The Strategy is composed of three pillars:

- Securing Government systems
- Partnering to secure vital cyber systems outside the federal Government
- Helping Canadians to be secure online

This document, the *Action Plan 2010-2015 for Canada's Cyber Security Strategy* (the Action Plan), outlines the Government's plan to implement the Strategy and meet our ultimate goal of securing our cyberspace for the benefit of Canadians and our economy. Substantial progress has been made to date with respect to the implementation of the Strategy. The Government has already completed many activities, for example:

- In 2011, the Government launched Shared Services Canada (SSC) to streamline the way we manage federal IT telecommunications, data centres, and email. The consolidation under SSC is making our information technology infrastructure more secure.
- In 2011, the Government clarified the roles and mandates for the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre (CCIRC), embedded at Public Safety Canada (PS), to improve Canada's ability to identify, prevent, and mitigate cyber security incidents.
- In 2011, the Government launched GetCyberSafe, our national public awareness campaign on cyber security that provides Canadians with the information they need to keep themselves and their families safe online.

- In 2012, the Government announced additional funding to reinforce federal Government IT infrastructure, which is vital to the protection of the information of Canadians, and information that underpins Canada's national security, public safety and economic prosperity. This funding is helping to strengthen Canada's already secure, stable and resilient digital infrastructure.

- In 2012, Canada signed a *Cyber Security Action Plan*, under the Beyond the Border Action Plan, with the United States (U.S.) in order to enhance the already strong partnership and cooperation on cyber security matters between both countries. This action plan recognizes the importance of protecting the shared critical digital infrastructure between Canada and the U.S., and of increasing our capacity to respond to cyber incidents.

- In 2012, the Government announced a new partnership between PS and STOP.THINK.CONNECT.™, a coalition of private sector companies, non-profit and Government organizations, including the U.S. Department of Homeland Security. This partnership will facilitate the alignment of public awareness campaigns in Canada and the U.S. and will provide citizens with important advice and tools to increase their online security.

- Canada also works closely with our other key security partners, the United Kingdom, Australia, and New Zealand, to ensure that our domestic and international efforts remain complementary. Canada is actively working to advance its cyber security interests at key international fora including NATO, the G8, as well as the United Nations and its associated agencies. Canada continues to conduct outreach to share information and knowledge to strengthen the cyber security capacity of foreign partners.

- The Government continues to engage critical infrastructure sectors (e.g. finance, transportation, energy), which are interconnected and spread out across Canada. To move forward with an integrated approach to engage this large stakeholder community, in 2010, PS and provincial/territorial partners launched the *National Strategy and Action Plan for Critical Infrastructure*. Together with *Canada Cyber Security Strategy*, these documents set out the national game plan to ensure that Canada's critical infrastructure sectors can respond and recover swiftly from incidents and disruptions, including cyber incidents.

- Finally, the Government has also taken steps to improve the collaboration between departments and agencies that are actively working to improve cyber security. Under the leadership of PS, new governance instruments have been established through a number of interdepartmental committees of senior officials.

The Action Plan demonstrates the Government's commitment to meet cyber threats head-on, with specific targeted actions aimed at producing significant, tangible results.

The Government continues to work with its partners in the provinces and territories, in the private sector, and internationally, in order to improve our collective cyber security. Cyber security is an issue of national importance for which, given the interconnected nature of our systems and networks, we have a shared responsibility and accountability.

Improving Governance

Many Departments and Agencies worked together to develop the Strategy. As the Government works with key partners to implement the Strategy, it needs to ensure that departments and agencies are working together effectively and efficiently to improve cyber security in Canada.

Implicated departments include:

- Canadian Forces;
- Canadian Security Intelligence Service;
- Canadian Radio Telecommunications Commission;
- Communications Security Establishment Canada;
- Defence Research and Development Canada;
- Department of Foreign Affairs and International Trade;
- Department of National Defence;
- Industry Canada;
- Justice Canada;
- Privy Council Office;
- Public Safety Canada;
- Royal Canadian Mounted Police;
- Shared Services Canada; and
- Treasury Board Secretariat.

Action	Timeline	Deliverable	Status	Lead
Improve Governance				
Provide leadership and coordination across Government in order to focus cyber security programs and resources.	Start: 2010	Introduce Canada's *Cyber Security Strategy*.	Completed	Public Safety Canada
		Implement Canada's *Cyber Security Strategy*.	Ongoing	Public Safety Canada

Action	Timeline	Deliverable	Status	Lead
Improve Governance (continued)				
Develop better governance within Government on cyber security.	Start: 2010	Establish interdepartmental governance mechanisms on Cyber Security.	Completed	Public Safety Canada
		Support these interdepartmental governance mechanisms.	Ongoing	Public Safety Canada
	Start: 2011	Establish a Government of Canada Security Governance Structure, consisting of a Lead Security Agency Steering Committee and a variety of working groups.	Completed	Treasury Board Secretariat
		Support the Government of Canada Security Governance Structure.	Ongoing	Treasury Board Secretariat
Improve collaboration within federal legal community on cyber security.	Start: 2011	Establish and operate a Justice Practice Group on Cyber Security.	Ongoing	Justice Canada
Provide the Government with timely and relevant metrics to measure the effectiveness of the efforts under *Canada's Cyber Security Strategy*.	Start: 2012	Develop a Horizontal Performance Measurement Strategy.	Completed	Public Safety Canada
		Evaluate *Canada's Cyber Security Strategy*.	On track to begin in 2015	Public Safety Canada

Pillar 1
Securing Government Systems

The Government is entrusted with safeguarding personal and business information in its electronic databases. It provides services to Canadians and the private sector through its websites and electronic processing systems, and transmits highly classified information that is essential to our military and to our national security operations.

Cyber incidents are directed at a range of computer networks, including Government systems, and those responsible for cyber incidents regularly probe these systems for vulnerabilities. Effectively securing these systems, and the data within them, is therefore a matter of national security and sovereignty.

The safekeeping of Canadians' personal information online, as well as the information technology infrastructure of the Government, is a priority. Measures have been put in place to provide secure online access to Canadians as the Government delivers more services. In addition, the Government is also consolidating its information technology infrastructure to further enhance its security.

The Government is working to strengthen its capability to detect, deter, and defend against cyber incidents while deploying cyber technology to advance Canada's economic and national security interests.

Action	Timeline	Deliverable	Status	Lead
Secure Government Systems				
Consolidate the Government's information technology security architecture, in order to improve the security of Government networks.	Start: 2011	Create Shared Services Canada to consolidate the Government's digital backbone.	Completed	Public Works and Government Services Canada
		Develop and implement new security standards for the procurement of information technology products and services for the Government.	Completed	Shared Services Canada, Public Works and Government Services Canada, and Communications Security Establishment Canada
Establish a mechanism to prevent and address sophisticated incidents on Government networks.	Start: 2011	Establish and operate the Cyber Threat Evaluation Centre at Communications Security Establishment Canada.	Fully operational	Communications Security Establishment Canada
Invest to reinforce the Government's cyber security capabilities.	Start: 2011	Invest $155 million over four years to hire new staff, and invest in better equipment.	On track for winter 2016	Various departments
	Start: 2012	Develop enterprise IT security architecture designs to ensure basic security building blocks are instilled as Government IT infrastructure is renewed.	Ongoing	Treasury Board Secretariat (in collaboration with Shared Services Canada and Communications Security Establishment Canada)
	Start: 2012	Deliver a new Government-wide IT security incident recovery capability to ensure timely response to and recovery from compromise.	Ongoing	Treasury Board Secretariat, Shared Services Canada, Communications Security Establishment Canada
	Start: 2012	Increase capacity to collect and analyze intelligence.	Ongoing	Communications Security Establishment Canada
	Start: 2012	Improve capacity to detect and defend against cyber threats.	Ongoing	Communications Security Establishment Canada
Strengthen military aspects of cyber security.	Start: 2010	Strengthen capacity to defend Department of National Defence/ Canadian Forces networks.	Ongoing	Department of National Defence/Canadian Forces
		Establish a Canadian Forces Cyber Task Force and Director General Cyber organization.	Completed	Department of National Defence/Canadian Forces
		Exchange information about cyber best practices with allied militaries.	Ongoing	Department of National Defence/Canadian Forces
Improve the Government's plan to respond effectively to a major cyber incident.	Start: 2009	Revise the Government's Information Technology Incident Management Plan.	Completed	Treasury Board Secretariat
Improve security training and awareness throughout the Government's security community.	Start: 2010	Lead and facilitate a variety of Government security community events, forums and training related initiatives.	Ongoing	Treasury Board Secretariat

Pillar 2
Partnering to secure vital cyber systems outside the federal Government

Canada's security and economic prosperity depend on the smooth functioning of systems outside the Government. Canada's private sector operates many of the systems, and is the custodian of sensitive information and industrial control systems, on which Canada's national security and public safety depend.

In addition, the ongoing success of Canada's private sector relies in large measure on its ability to commercialize innovative research and intellectual property, business transactions, and financial data. Failing to secure this vital digital information, and the systems that hold it, inevitably leads to lost market share, fewer customers and corporate breakdown for the companies involved. On a national scale, the theft of trade secrets, intellectual property and confidential corporate information can result in lost jobs and diminished economic prosperity for Canada and Canadians.

Many of the risks and impacts of cyber incidents are shared between governments and the private sector. Fortunately, Canada's public and private sectors share a long history of working together to achieve shared economic and national security objectives. This cooperation needs to be further strengthened.

Strengthened partnerships among all levels of Government are also essential in order to deliver a comprehensive cyber security strategy for Canada and Canadians. Our provincial and territorial counterparts provide a range of essential services whose delivery is dependent on the safe and secure operation of their cyber systems.

The disruption of critical infrastructure and cyber systems can have direct impacts on businesses and communities around the world. Incidents on interconnected cyber networks can have cascading effects across industrial sectors and national borders. At the same time, Canada needs to be active in international fora dealing with critical infrastructure protection and cyber security.

Action	Timeline	Deliverable	Status	Lead
Work With Partners Outside the Government of Canada				
Develop a new process to coordinate a national response to major cyber incidents.	Start: 2012	Develop a Cyber Incident Management Framework.	On track for fall 2013	Public Safety Canada
Engage owners and operators of Canada's critical infrastructure, using the mechanisms established under the National Strategy and Action Plan for Critical Infrastructure.	Start: 2010	Provide cyber security briefings to all sector networks.	Ongoing	Public Safety Canada
	Start: 2013	Develop and implement a strategy to engage CEOs on cyber security.	On track for spring 2013	Public Safety Canada
Engage provinces and territories on cyber security, to seek their active engagement in improving the cyber security of their systems and vital systems under their jurisdiction.	Start: 2011	Establish the Federal Provincial and Territorial Assistant Deputy Minister Committee on cyber security.	Completed	Public Safety Canada
		Obtain security clearances for, and provide classified briefs to the National Chief Information Officer Sub Committee on Information Protection which includes provinces and municipal representatives.	Completed	Public Safety Canada
		Develop and implement information sharing arrangements and protocols.	Ongoing	Public Safety Canada
	Start: 2001	Operate a Federal/Provincial/Territorial Coordinating Committee of Senior Officials Cyber Crime Working Group.	Ongoing	Justice Canada
Develop a Cyber Security Partnership Program for vital systems outside the Government to provide tangible support to their owners and operators.	Start: 2010	Organize workshops across the country to improve awareness and understanding of the threats to industrial control systems.	Ongoing	Public Safety Canada and Royal Canadian Mounted Police
		Establish an Industrial Control System laboratory program and testing environment – the National Energy Infrastructure Test Center.	Completed	Public Safety Canada, Natural Resources Canada, Royal Canadian Mounted Police, and Defence Research and Development Canada
		Operate the Industrial Control System laboratory program and testing environment.	Ongoing	Public Safety Canada, Natural Resources Canada, and Defence Research and Development Canada
		Develop and implement a grant and contribution program.	On track for spring 2013	Public Safety Canada
		Design and implement other program elements, in consultation with owners and operators of vital systems.	Ongoing	Public Safety Canada

Action	Timeline	Deliverable	Status	Lead
Improving the Canadian Cyber Incident Response Centre's (CCIRC) Ability to Support Systems Outside the Government of Canada				
Increase capacity of CCIRC	Start: 2012	Increase the operating hours of CCIRC to 15 hours per day, seven days per week to correlate with business hours coast-to-coast.	Completed	Public Safety Canada
	Start: 2011	Invest in CCIRC's technical capability, through training, analytical systems and processes, automation and technology.	Ongoing	Public Safety Canada
Improve the capabilities of CCIRC, in order to assist owners and operators of vital systems to improve their cyber security posture.	Start: 2011	Refine and update CCIRC's mandate to focus on delivering products and services to vital systems outside the Government of Canada.	Completed	Public Safety Canada
		Update CCIRC's standard procedures and policies to provide a high and consistent level of support to clients, in light of expanding operations.	Ongoing	Public Safety Canada
		Launch CCIRC's Community Portal within the Critical Infrastructure Gateway.	Completed	Public Safety Canada
		Operate CCIRC's Community Portal.	Ongoing	Public Safety Canada
		Establish personnel exchange between CCIRC and the Communications Security Establishment Canada.	Completed	Public Safety Canada and Communications Security Establishment Canada
		Commission significant test facilities to improve CCIRC's ability to perform technical research and analysis.	Completed	Public Safety Canada
Identify and assess gaps in policy with respect to cyber security in Canada.	Start: 2011	Provide advice to Government.	Ongoing	Public Safety Canada
Promote Research and Development				
Support cyber security research and development activities in order to enhance the technical tools to improve cyber security.	Start: 2011	Provide funding to the innovation system, including academic institutions, to develop new technological solutions for cyber security.	Ongoing	Defence Research and Development Canada
Develop an academic engagement program for cyber security, to promote the development of a strong and cohesive academic community in the social sciences dimension of cyber security.	Start: 2012	Host an academic workshop on Critical Infrastructure and Cyber Security issues.	Completed	Public Safety Canada
		Commission research papers on cyber security.	Ongoing	Public Safety Canada

Action	Timeline	Deliverable	Status	Lead
Engage the International Community				
Develop a Canada-U.S. Action Plan on cyber security that will bolster Canadian capabilities and improve the cyber security of our shared infrastructure.	Start: 2012	Develop the Canada-U.S. Action Plan on Cyber Security, under the Beyond the Border Action Plan.	Completed	Public Safety Canada
	Start: 2010	Implement the Canada-U.S. Action Plan on Cyber Security.	Ongoing	Public Safety Canada
Work with close allies and partners to promote Canada's interest in a cyberspace that is open, interoperable, secure, and reliable.	Start: 2010	Permanently assign diplomatic personnel for Canada in the United Nations offices in Geneva to deal specifically with cyber security issues.	Completed	Department of Foreign Affairs and International Trade
		Position Canada as one of the 15 nations working to prepare a major United Nations study for the Secretary of the United Nations.	Completed	Public Safety Canada, Department of Foreign Affairs and International Trade, and Department of National Defence/ Canadian Forces
		Undertake regular policy and operational collaboration internationally.	Ongoing	Public Safety Canada, Department of Foreign Affairs and International Trade and Department of National Defence/ Canadian Forces
Work with international organizations and foreign Governments to improve their cyber security capabilities, thereby improving Canada's ability to keep our shared infrastructure safe.	Start: 2012	Undertake capacity building with a number of regional partners including the Organization for Security and Cooperation in Europe, the Association of Southeast Asian Nations Regional Forum and the Organization of American States (OAS).	Ongoing	Department of Foreign Affairs and International Trade and Public Safety Canada
		Host an OAS workshop to share best practices on the development of national cyber security strategies.	Completed	Public Safety Canada
Develop a framework to ensure that activities in cyberspace are aligned with broader foreign policy, international trade and security objectives.	Start: 2012	Create a cyber security foreign policy.	On track for fall 2013	Department of Foreign Affairs and International Trade
Improve Government communication and collaboration on international cyber issues.	Start: 2011	Establish and operate the Inter-departmental Working Group on International Cyber Issues.	Ongoing	Rotating chair between Department of Foreign Affairs and International Trade, Public Safety Canada, Justice Canada, and Industry Canada
Engage with international partners to study the United Nations' work on cyber crime.	Start: 2010	Work on cyber crime study by the United Nations. Represent Western European and Other Governments as Rapporteur (Justice Canada).	Ongoing	Justice Canada and Department of Foreign Affairs and International Trade

Pillar 3
Helping Canadians to be secure online

The third pillar of *Canada's Cyber Security Strategy* focuses on providing Canadians with information to protect themselves and their families online, and on strengthening the ability of law enforcement agencies to combat cyber crime.

Action	Timeline	Deliverable	Status	Lead
Improve Public Awareness				
Help Canadians to be secure online.	Start: 2011	Develop a strategy that includes advertising, partnerships, web, social media, proactive media relations, earned media, parliamentary engagement, exhibits/special events, and internal communications plans.	Completed	Public Safety Canada
		Implement the communication strategy.	Ongoing	Public Safety Canada
	Start: 2011	Conduct baseline public opinion research to evaluate Canadians' cyber security awareness, attitudes, and behaviours.	Completed	Public Safety Canada
	Start: 2011	Establish a national public awareness campaign, Get Cyber Safe, with web, social media and media activities with the website, GetCyberSafe.ca as a focal point.	Ongoing	Public Safety Canada
	Start: 2011	Build partnerships with other federal organizations, as well as domestic and international stakeholders, to increase the reach, frequency and impact of messaging to target audiences.	Ongoing	Public Safety Canada

Action	Timeline	Deliverable	Status	Lead
Improve Public Awareness (continued)				
Help Canadians to be secure online. *(continued)*	Start: 2011	Partner with STOP.THINK. CONNECT.™ (a coalition of private sector companies, non-profit and Government organizations, including the Department of Homeland Security, committed to informing the public about how to stay safer online).	Ongoing	Public Safety Canada
	Start: 2012	Conduct secondary analysis of cyber security threat environment to inform public awareness campaign.	Ongoing	Public Safety Canada
Cyber Crime				
Create a Cyber Crime Fusion Centre to advance situational awareness and analysis of cyber crime trends, including new methods for performance measurement and statistical collection.	Start: 2011	Establish the Cyber Crime Fusion Centre.	Completed	Royal Canadian Mounted Police
		Develop the first report by analyzing cyber crime trends and methods.	On track for fall 2013	Royal Canadian Mounted Police
Draft a Canadian Cyber Crime Strategy.	Start: 2012	Draft a Cyber Crime Strategy to deal with all aspects of cyber criminality, including fraud, organized crime and identity theft.	Ongoing	Royal Canadian Mounted Police
Improve the legislative tools to better protect Canadians in cyberspace.	Start: 2010	Bill C-12, *Canada's Anti-spam Legislation.*	Royal Assent received but Act not yet in force	Industry Canada
	Start: 2011	Bill C-12, *Safeguarding Canadian's Personal Information Act*, which includes data breach notification requirements for organizations.	Ongoing (awaiting Second Reading)	Industry Canada

Conclusion

Cyber security is a shared responsibility, and requires close partnership between the federal Government, the private sector, other levels of government, international partners, and Canadians to ensure that vital cyber systems are secure, and that Canadians can go online with confidence. The Strategy and the Action Plan reflect this shared responsibility. Going forward, to ensure continued progress, this Action Plan will be reviewed and updated periodically in collaboration with partners within and outside the federal government.