Public Safety Canada | Sécurité publique Canada

Public Safety Canada

Horizontal Evaluation of Canada's Cyber Security Strategy

Final Report

2017-09-29

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Program

Canada's Cyber Security Strategy (CCSS) was released on October 3, 2010, to outline the federal government's plan to secure Canada's cyber systems and protect Canadians online. The Strategy is built on three pillars: securing Government of Canada systems; partnering to secure vital cyber systems outside the Government of Canada; and helping Canadians to be secure online. The first pillar commits to placing necessary structures, tools and personnel to strengthen Government of Canada's ability to prevent, detect, respond to, and recover from cyber threats. The second pillar commits to working with provincial and territorial governments as well as the private sector to support initiatives that strengthen Canada's cyber resiliency, including the critical infrastructure sectors. The third pillar commits to promoting public awareness and education to help Canadians protect themselves and their families online. In addition, this pillar looks to strengthen the ability of law enforcement agencies to combat cybercrime. The CCSS is implemented by nine Government of Canada organizations and the ongoing funding for all partners combined is slightly more than $60 million per year.

Why it is important

Canadians are increasingly embracing cyberspace and the Canadian economy relies heavily on the Internet. Although this presents Canadians with tremendous benefits and opportunities, it can also open them up to threats. As a result, it is important for Canada and Canadians to anticipate and confront emerging threats arising from cyber activities. The activities carried out under Canada's Cyber Security Strategy were intended to ensure that Canadians could maximize the benefits that cyber space and technologies have to offer, while mitigating any associated risks.

What we examined

This evaluation was conducted in fulfilment of the requirements of the *Financial Administration Act* and the Treasury Board of Canada 2016 *Policy on Results*. The evaluation assessed the extent to which the horizontal governance structure was effective in overseeing the Strategy's implementation; the extent to which participating departments and agencies implemented the Strategy's funded activities; and the extent to which planned activities contributed to achieving the Strategy's main objectives.

What we found

Governance

The evaluation found that the governance structure facilitated collaboration, coordination, and information-sharing among participating organizations. However, due to lack of documentation, the evaluation was unable to determine the extent to which the oversight committees fulfilled their stated purposes as outlined in their terms of reference. For example, in accordance with their terms of reference, the oversight committees, particularly the Deputy Minister (DM) Cyber Committee, were to meet on a regular basis to provide strategic advice and to monitor progress

on the implementation of the Strategy. The evaluation was unable to determine to what extent these roles and responsibilities were fulfilled as the meeting minutes were not kept on a consistent basis.

The evaluation also concluded that information sharing was done on an ad hoc or selective basis and that there was no clear policy on what should be shared, with whom, and when. Currently, there is no efficient mechanism for sharing classified information, particularly in real time.

The Strategy helped clarify roles and responsibilities of Government of Canada organizations by putting in place a management framework to clarify objectives, assign roles and responsibilities, and establish various committees and working groups. However, the evaluation identified specific instances where perception of overlapping roles and responsibilities caused confusion and frustration for federal departments, agencies, and private sector stakeholders.

Performance - Implementation

The evaluation found that most of the Strategy-funded activities were implemented as intended. However, there were at least four activities that were not fully implemented: Defence Research and Development Canada's (part of National Defence) activity to develop an enterprise architecture and its related deliverables; the RCMP's activity to publish an annual report on cybercrime; Shared Services Canada's activities to secure a Third Internet Connection and to establish a Cyber Infrastructure Recall System.

Some of the participating organizations faced difficulties providing relevant performance information which may indicate that such information was not being collected regularly and consistently. Three organizations have reported under-spending of the allocated funding, two organizations spent more, two the exact amount and one was unable to track its relevant expenditures. Since the oversight committees did not keep meeting minutes on a consistent basis, the evaluation was unable to determine to what extent the oversight committees, particularly the DM Cyber Committee, were kept informed of these delays in implementation in order to fulfill their stated purposes in monitoring progress on the implementation of the Strategy.

Performance - Effectiveness

The evaluation found that the Strategy contributed towards increasing the Government of Canada's capacity to prevent, detect, respond to, and recover from cyber attacks. In particular, the Strategy helped improve the ability of government organizations to quickly analyze and contain data breaches. While cyber incidents and breaches still occur, they are becoming less frequent. These improvements were noted despite an increase in state- and non-state-sponsored cyber activities against Government of Canada networks in recent years. Nevertheless, interviewees noted that there are further opportunities for improvements.

The evaluation also found that the Strategy contributed towards fostering partnerships with critical infrastructure owners and operators as well as other private sector stakeholders. However, interviewees and the literature suggested that the overall progress of partnering to secure vital cyber systems outside the Government of Canada has been limited. In particular, the Strategy's overall investment in securing cyber systems of importance to Canada was described as

inadequate and there has been limited progress in establishing reciprocal norms for information sharing with the private sector as well as with provinces and territories.

Finally, there is a perception among the majority of interviewees that Canadians are more aware of cyber threats today compared to the past. However, it is unclear whether this increased awareness can be attributed to CCSS or if it has made Canadians safer online.

Given these findings, the evaluation has identified a number of opportunities for improvement and has put forward recommendations to address them. As the lead organization, Public Safety has made a commitment to address these issues, in collaboration with partner organizations, as part of the efforts to renew Canada's Cyber Security Strategy to better prepare Canada to improve its national, economic and cyber security position.

Recommendations

In collaboration with participating organizations, the Senior Assistant Deputy Minister of the National and Cyber Security Branch, Public Safety, should consider undertaking the following:

1) Strengthen horizontal governance of cyber security in the Government of Canada by:
    a. re-assessing the governance structure to determine the need and demand for the current committee configuration and to improve participation;
    b. improving the provision of secretariat support, including coordination, information management and other administrative services;
    c. ensuring that governance committees have terms of references that clearly define roles, responsibilities, and expectations from members;
    d. ensuring that the oversight committees fulfill their roles and responsibilities as outlined in each oversight committee's terms of reference; and
    e. keeping meeting minutes on a consistent basis.

2) Strengthen the Cyber Security related information–sharing practices by developing policies, procedures and tools to ensure timely and systematic exchange of information among partners and stakeholders.

3) Strengthen the Strategy's performance measurement and data collection practices by:
    a. collecting relevant, reliable and outcome oriented performance information, including information on program expenditures, on a regular and consistent basis; and
    b. providing performance and expenditure information collected to the appropriate oversight committees on a regular basis to support effective monitoring and accountability.

Management Response and Action Plan

Management accepts all recommendations and will implement an action plan.

1. INTRODUCTION

This report presents the findings of the Public Safety Canada's Horizontal Evaluation of Canada's Cyber Security Strategy (CCSS).

The evaluation was conducted to provide Canadians, parliamentarians, Ministers, central agencies, and the Deputy Ministers of the participating organizations with an evidence-based, neutral assessment of the governance, implementation and performance of the Strategy. It was conducted in compliance with the Treasury Board of Canada 2016 *Policy on Results*.

It should be noted that the Minister of Public Safety is mandated by the Prime Minister, in collaboration with his counterparts at the Department of National Defence, Infrastructure and Communities, Public Services and Procurement Canada, Innovation, Science and Economic Development, and the Treasury Board of Canada Secretariat, to conduct a review of existing measures to protect Canadians and the critical infrastructure from cyber-threats. The evaluation findings are intended to complement this process and inform future cyber security related policy renewal efforts of the Government of Canada.

Released on October 3, 2010, the Strategy outlined the Government of Canada's response to the growing need to secure Canada's cyber systems and protect Canadians online.[1] To that end, the Strategy laid out the Government of Canada's plan to secure its cyber systems, as well as its vision for partnering with the provinces and territories, the private sector (including critical infrastructure owners and operators), academia, international allies, and individual Canadians to address threats to cyber security in Canada.

The Strategy was based on three pillars:

- Securing Government of Canada Systems—intended to strengthen the Government of Canada's ability to prevent, detect, respond to, and recover from cyber threats.
- Partnering to Secure Vital Cyber Systems Outside the Government of Canada—meant to strengthen cyber resiliency in Canada, including that of critical infrastructure sectors.
- Helping Canadians to be Secure Online—intended to promote public awareness, educate Canadians on how to protect themselves, and strengthen the ability of law enforcement agencies to combat cybercrime.

Annex A describes at a high level the roles and responsibilities of the Government of Canada organizations under each pillar.

[1] Cyber security is defined as the protection of digital information and the infrastructure on which it resides from "unauthorized access, use, manipulation, interruption or destruction via electronic means" (CCSS, Page 3).

The Strategy sought to achieve three key outcomes:

- Government of Canada systems are secure;
- systems of importance to the Government of Canada are secure; and
- Canadians are safe and secure online.

The Evaluation covers the activities of nine Government of Canada organizations that were involved in the implementation of the Strategy: Public Safety (PS), Communications Security Establishment (CSE), Shared Services Canada (SSC), Department of National Defence/Defence Research and Development Canada (DND/DRDC), Treasury Board of Canada Secretariat (TBS), Global Affairs Canada (GAC), Justice Canada (JUS), the Royal Canadian Mounted Police (RCMP), and Canadian Security Intelligence Services (CSIS).

1.1 Horizontal Governance and Oversight

Public Safety Canada provides national leadership and coordination, notably in the implementation of Canada's Cyber Security Strategy, including the advancement of national cyber security policy. Public Safety Canada leads the coordination of the Government's efforts to protect Canada's critical infrastructure and Canadians, and is responsible for cyber emergency management. In collaboration with its federal, domestic, and international security partners, Public Safety coordinates an integrated national strategic approach to cyber security, and through the Canadian Cyber Incident Response Centre (CCIRC),[2] and where required, the Government Operations Centre (GOC), the national response to cyber events of national interest. [3]

Public Safety leverages the Deputy Minister, Assistant Deputy Minister, and Director General Committees on Cyber Security to steer the implementation of the Strategy and resolve issues as they arise. These senior management committees are intended to provide strategic guidance as required to ensure the timely and efficient roll out of the Strategy.

Table 1: Governance structure for the implementation of Canada's Cyber Security Strategy[4]

Cabinet												
Deputy Ministers Committee on Cyber Security (DM Cyber)												
Assistant Deputy Ministers Committee on Cyber Security (ADM Cyber)												
Directors General Committee on Cyber Security (DG Cyber)							**Directors General Committee on Cyber Security Operations (DG Cyber Ops)**					
PS	**CSIS**	**RCMP**	**DND**	**CSE**	**DND/DRDC**	**GAC**	**JUS**	**PSPC[5]**	**SSC**	**TBS**	**PCO[6]**	**ISEDC[7]**

[2] CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents. As such, it is considered Public Safety's operational arm.

[3] 2012 Inception Document, page 7, paragraph 3 and page 37, paragraph 91.

[4] Note that not all listed organizations in the above-table are members of all committees.

[5] PSPC is responsible for, among other things, maintaining relationships with allies and negotiating memoranda of understanding on industrial security matters, including cyber security, in contracting.

2. ABOUT THE EVALUATION

2.1 Evaluation Overview

This evaluation was conducted to fulfill the requirements of the *Financial Administration Act* and the Treasury Board of Canada *Policy on Results* (2016).

The evaluation's main objective was to assess the extent to which:

- the horizontal governance structure was effective in delivering the Strategy, including providing oversight and clarifying the roles and responsibilities of various partners;
- the participating departments and agencies implemented the Strategy's prescribed activities; and
- the planned activities contributed to achieving the Strategy's main objectives.[8]

The evaluation covered activities undertaken between 2010−11 and 2015−16. The data collection and analysis phases of the evaluation were carried out between May and September 2016.

2.2 Methodology

The evaluation employed the following lines of evidence:

Literature review—comprised a web-based search of documents related to broad topics on cyber security in general, and Canada's Cyber Security Strategy in particular.

Document review—included reviewing inception documents, performance reports, financial information, and recent audit reports. These reports included the Office of the Comptroller General's 2015 *Horizontal Audit of Information Technology Security in Large and Small Departments*.

Interviews—involved conducting 48 interviews with government officials from 11 Government of Canada organizations, as well as academics and other experts. Participating organizations determined at their discretion who and how many to interview.

---

[6] PCO is responsible for housing and providing support to the National Security Advisor to the Prime Minister, coordinating activities of the Canadian security and intelligence community and promoting a coordinated approach to national security issues.

[7] ISEDC is responsible for fostering a robust and reliable telecommunications system, developing policies to ensure a safe and secure online marketplace and the continuity of telecommunications during an emergency.

[8] In an effort to minimize duplication, the evaluation did not assess the relevance of the Strategy (i.e., continued need, linkages to government priorities and departmental strategic outcomes and alignment with federal roles and responsibilities) as these issues were expected to be covered by the above-mentioned Cyber Review.

Table 2: Stakeholder groups and number of interviews

Interviewee Group			Number of Interviews
Participating departments and agencies	*Organization*	*Number*	42
	PS	4	
	RCMP	6	
	JUS	6	
	DND/DRDC	1	
	CSE	9	
	TBS	4	
	SSC	4	
	CSIS	4	
	GAC	4	
Other government departments	ISEDC	1	2
	PSPC	1	
External to government subject matter experts and academics			4
TOTAL			**48**

Performance and financial information was collected, reviewed, and analyzed to supplement information collected through other lines of evidence.

2.3 Limitations

The quality and availability of performance information varied among partners. Where performance information was lacking, the evaluation team supplemented the data with interviewee perceptions and document review.

Expenditure related information was provided to us by each participating organization. The evaluation did not independently verify the validity of the information provided.

We made several attempts to interview officials from private sector organizations. However, these officials were unavailable to comment or did not respond to our requests for an interview.

The scope of the evaluation was limited to certain activities undertaken between 2010 and 2016. It is important to note that there have been many other funded and unfunded activities that have been undertaken by Government of Canada organizations in support of the Strategy. Although the evaluation made it clear that it was only assessing the contribution of these particular activities, it is not possible to measure or isolate *the exact attribution* of a group of activities to the achievement of the Strategy's overall objectives.

2.4 Evaluation Questions

Annex B contains a list of questions addressed in the evaluation.

3. EVALUATION FINDINGS

3.1 Governance

This section addresses governance-related questions such as: to what extent has the horizontal governance structure been effective? Are the roles and responsibilities of each participating organization clearly defined and adhered to? And what is the state of information-sharing, collaboration and coordination among partners? There is also a brief discussion on the state of cyber security research and development.

Evaluation Finding: Although the governance structure facilitated, to some extent, collaboration, coordination and information-sharing among participating organizations, the absence of meeting minutes, other documentation or staff with corporate memory limited the evaluation's ability to assess the governance structure's overall effectiveness and the extent to which the oversight committees fulfilled their stated purposes.

3.1.1 Effectiveness of Governance Committees

The Strategy employed decentralized governance, which was in-line with the structure of most horizontal initiatives in the Government of Canada. Under this governance approach, although Public Safety was given the responsibility to coordinate the overall activities, participating organizations are accountable only to their own Ministers, who are, in turn, accountable to Parliament.

While some interviewees argued that this structure reinforced the culture of working in silos, the majority believed that it was effective in creating opportunities for closer collaboration among participating organizations. Public Safety was to fulfill its coordination responsibility through a governance structure that included various oversight committees, including the DM, ADM, DG Cyber and DG Cyber Operations[9] Committees, as well as many working level communities of practice.[10]

[9] The DG Cyber Operations Committee was established to ensure that there was coordination in confronting cyber threats and incidents of national interest and that national operational policy issues are advanced. It was differentiated from the DG Cyber Committee by its operational focus. The Committee's membership consisted of those government departments that have an operational role inside and/or outside of the federal government including but not limited to: PS, CSE, CSIS, DND, SSC, the RCMP, and the Canadian Radio-television and Telecommunications Commission.

[10] There are other pillar specific senior management and working level committees and working groups that are established to further IT security in general and achieving the objectives of the Strategy in particular. However, this evaluation has only examined the government-wide governance structure and governance committees as described in the Strategy-related official documents, including the Strategy's performance measurement framework.

At least three committees (DM Cyber, DG Cyber, and DG Cyber Operations) established terms of references in writing. According to these terms of references, these Committees were responsible, among other things, to "monitor progress on the implementation of *Canada's Cyber Security Strategy*." The DM Cyber Committee and DG Cyber Committee were to meet once every two months and the DG Cyber Operations Committee every two weeks or as required in response to operational matters; however, it appears that only the DG Cyber Operations Committee met regularly.

Based on the information received, none of the committees appear to have kept meeting minutes on a consistent basis.

The DG Cyber Operations Committee was described by the majority of the interviewees to be effective and a good forum for exchanging information among participating organizations. However, it was also observed by some of the interviewees that the Committee's membership needs to be expanded to include additional Government of Canada cyber stakeholders such as the Treasury Board Secretariat. Some concerns were also expressed that the Committee had lost robustness over the past year as members increasingly sent delegates to meetings.

In addition to this formal structure, various working level communities of practice evolved and met more regularly than their parent committees to share information and discuss issues. Although vibrant, these communities did not have direction-setting power and tended to depend heavily on specific people. As a result, personnel changes affected the communities' working relationships and effectiveness.

According to its Terms of Reference, the DM Cyber Committee was to establish policy directions, set cyber security related priorities for member organizations and monitor progress on the implementation of the Strategy. However, given the absence of consistent meeting minutes, other documentation or staff with corporate memory, the evaluation was unable to assess the extent to which the Committee was able to fulfill these responsibilities.

Observations and Opportunities for Improvement

The evaluation identifies strengthening the governance structure as an opportunity for improvement. To that end, the composition of the governance structure needs to be reconfigured and its operations formalized, including the operations of the oversight committees. This formalization could include, among other things:

- improving the provision of secretariat services;
- establishing terms of reference for each oversight committee that clearly define roles, responsibilities, and expectations from members;
- meeting regularly in accordance with each oversight committee's terms of reference; and
- keeping meeting minutes on a consistent basis.

In addition, given the evolution of cyber security and its increased significance for Canada's economic prosperity, there is a need for holding senior management level meetings to regularly

discuss strategic cyber-related issues, including international aspects of cyber security (e.g., cyber foreign policy).

3.1.2 Clarity of Roles and Responsibilities

Before the Strategy was established, the cyber security related roles and responsibilities of Government of Canada organizations were unclear.[11] There were no clear processes and mechanisms for information sharing, particularly with security and law enforcement agencies.

The Strategy put in place a management framework to clarify objectives, assign roles and responsibilities, and establish various committees/working groups such as the DM, ADM, DG Cyber and DG Cyber Operations Committees to assist Government of Canada organizations to share information, collaborate, and coordinate with one another.

Organizing the Strategy under three distinct, but complementary, pillars helped clarify each partner's roles and responsibilities. Furthermore, the roles and responsibilities of each organization were further explained in documents such as: *Government of Canada Cyber Security Event Management Plan*,[12] *the Federal Emergency Response Plan*[13] and the *Cyber Incident Management Framework for Canada*.[14]

Although through the publication of these documents and other efforts the roles and responsibilities of various players have been clarified over the years, a number of interviewees identified specific instances of mandate overlap and lack of clarity in roles and responsibilities that at times caused confusion and frustration for the departments and agencies involved, as well as their private sector stakeholders. For example:

- In some instances, two or three government organizations attended meetings with critical infrastructure and/or private sector organizations without having first harmonized the Government's messages. This lack of coordination in messaging was also observed within Public Safety, in particular between cyber security and critical infrastructure groups.
- Several Government of Canada organizations have proclaimed (and even can proclaim today) that they are the single point of contact for the private sector in the case of an incident.
- Different partner organizations developed software or other tools to address a cyber-related issue not realizing that another partner organization had either developed or were in the process of developing the same software or tools.

[11] This statement may not apply to the RCMP as it has indicated that its roles, responsibilities and authorities with respect to cyber security have always been clear.

[12] https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

[13] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-en.aspx.

[14] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-en.aspx#_Toc360619103.

There is a perception both among some of the interviewees and the private sector stakeholders with whom they have been in contact that the roles, responsibilities, and mandate of the Canadian Cyber Incident Response Centre overlap, to some extent, with those of CSE.[15,16]

Accordingly, critical infrastructure owners and operators were particularly unclear about the roles and responsibilities of these two organizations. This lack of clarity exists despite attempts in recent years to focus the mandates of the two organizations: CSE was to address issues related to systems of importance to Canada, and the Canadian Cyber Incident Response Centre was to play more of a coordination role in information-sharing and incident management. Several interviewees indicated that many in the private sector were unclear which organization should serve as their point of contact for cyber issues.[17]

Observations and Opportunities for Improvement

As the context for cyber security has evolved, there is a need to redefine roles and responsibilities of government entities, particularly with respect to identifying and communicating to the private sector a single point of contact for all cyber related incidents.[18]

In addition, given the growing economic significance of cyber security, there is a need to clarify what should be the appropriate roles, responsibilities, and level of involvement of departments with economic portfolio, such as Innovation, Science, and Economic Development Canada in cyber security.

3.1.3 State of Coordination and Collaboration

Most interviewees described Public Safety as being well positioned to coordinate the cyber security file. However, the Department's authority is limited to its persuasion power, and to some extent, to having the lead on policy renewal processes.[19]

---

[15] Communications Security Establishment (CSE) is mandated to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties and is the communications security (COMSEC) authority for Canada, which includes auditing COMSEC doctrine (https://www.cse-cst.gc.ca/en/inside-interieur/what-nos).

[16] This evaluation did not investigate whether such overlap did in fact exist between the mandates of CCIRC and the CSE.

[17] A document entitled *Cyber Incident Management Framework for Canada* identifies CCIRC, in most cases, as the first point of contact in the Government of Canada for an affected organization. At the same time, the document instructs affected organizations to contact local law enforcement authorities if the organizations believe that a crime has been committed or to contact CSIS should the organizations believe that national security is threatened. If in doubt, the affected organizations are asked to contact CCIRC. These varying options could partially explain why some interviewees were unclear whom critical infrastructure owners and operators and other private sector organizations should contact first in the Government of Canada when facing a security incident.

In addition, some interviewees external to the Government of Canada also indicated that the private sector does not clearly understand Public Safety's role. In their experience, in the case of a cyber-incident, affected organizations are more likely to turn to the RCMP or CSE than to Public Safety, given their relative unfamiliarity with Public Safety's role.

[18] Note that those interviewees who raised this issue did not define what they meant by "cyber incidents". However, it is the evaluators' assumption that they were referring to those incidents for which there are no well-established reporting practices/protocols in place.

Nevertheless, Public Safety was believed to be doing a good job in coordinating the Strategy-related activities, particularly at the working level. However, several interviewees noted a disconnect between the operations and policy sides. For example, some of the organizations that are only involved in policy argued that they are often unaware of developments in operations.

Accordingly, this disconnect has led to the creation of two parallel structures, one around policy and strategic issues and another around operational issues. This split was argued to have undermined the horizontality of the Strategy. Some departments and agencies involved only in policy argued that because of their mandates, they should be also involved in operations; conversely, others involved solely in operations believed that they had not been informed about policy developments.

The Strategy considered provinces and territories as important partners in securing cyber space for Canadians. To this end, a Federal/Provincial/Territorial Deputy Ministers' Table on cyber security was created to help the Government of Canada collaborate and share information with provinces and territories. However, these expected results proved elusive. For various reasons, it was found to be challenging to hold policy discussions among stakeholders and to agree how to proceed on given issues, including information-sharing. Those involved found, in practice, classified information-sharing is extremely limited, declassifying information is difficult, and establishing efficient systems to share information requires investment from the recipient as much as from the Government of Canada.

The creation of Shared Services Canada, which consolidated information technology (IT) infrastructure within the Government of Canada, was described by some of the interviewees to have further facilitated collaboration on cyber security among Government of Canada organizations.[20]

3.1.4 Facilitators and Impediments to Information Sharing

Information sharing improved over the years among participating departments and agencies, as well as with non-government stakeholders, including critical infrastructure owners and operators and other private sector stakeholders.

Various formal and informal mechanisms have been put in place to share information. For example and as indicated elsewhere in this report, prior to the advent of the Strategy there was no clear mechanism to share information with intelligence and law enforcement agencies. The Strategy-established oversight committees provided a forum for participating organizations to share information, particularly at the operational level. The Canadian Cyber Incident Response Centre has also put mechanisms in place to share information, issue alerts and advisories to

[19] The Strategy's Performance Measurement Framework identified the "lack of central authority" as one of the risks that may impede both the implementation and success of the Strategy (page 19).

[20] The Government of Canada created Shared Services Canada on August 4, 2011, to transform how the Government manages its information technology infrastructure. Shared Services Canada is mandated to deliver email, data centre and telecommunication services and related Cyber and IT Security services to 43 federal departments and agencies. It also provides other optional services to government departments and agencies on a cost-recovery basis. Note that currently more than 50 government organizations remain outside the purview of Shared Services Canada.

inform critical infrastructure organizations, businesses and provincial/territorial/municipal partners of potential, imminent or actual cyber threats, incidents and vulnerabilities.

Despite improvements made, for the most part information sharing among participating organizations was done on an ad hoc and selective basis. There was no clear policy as to what should be shared, with whom and when. It was mostly the individual organizations that decide on their own terms what to share with others. Although competing and/or differing mandates impeded information sharing in some instances, work volume and tight timelines proved the biggest obstacles to collaboration and information sharing. In other words, organizations lacked the time, not the will, to share information.

There is a lack of appropriate tools and infrastructure for sharing classified information. Currently, several classified networks across government lack interoperability. In addition, only a limited number of employees have access to these networks.

Observations and Opportunities for Improvement

Information sharing needs to become systematic and formalized; it should be clear what information should be shared, who should share it, and when it should be shared, with consideration of legal and policy parameters.

There is also a need to improve the infrastructure for sharing and exchanging classified information. For example, the Government of Canada needs to build communications infrastructure that is more interoperable and secure, and provide more employees with access to secure networks.[21]

3.1.5 State of Cyber Security Research and Development (R&D)

The Strategy prompted some limited R&D investment, particularly in Pillar I—Securing Government of Canada Systems. Most of the funded research was applied research meant to provide benefits within one to five years.[22]

Some of the organizations participating in Canada's Cyber Security Strategy faced difficulty staffing certain highly technical positions. In addition, the existing cyber security workforce was described to be over-extended. These issues were cited as evidence that Canada needs to develop more and better capacity in cyber security and that Canadian universities and colleges need to produce more graduates with cyber security skills.

---

[21] Shared Services Canada, in collaboration with Privy Council Office, Treasury Board of Canada Secretariat and Communications Security Establishment, has implemented an interim Government of Canada Secret Infrastructure service in a limited capacity and is currently working to provide this central service to a much larger audience within the Government of Canada (contingent on funding).

[22] The Government of Canada has funded a number of cyber security research and development projects through other initiatives. For example, the Canadian Safety and Security Program, co-managed by the Department of National Defence and Public Safety Canada includes an e-Security Portfolio whose science and technology projects are intended to contribute to securing systems of importance to the government of Canada and helping Canadians be more secure online.

Observations and Opportunities for Improvement

The Government of New Brunswick was noted by some of the interviewees and in the literature as a successful example of a government nurturing a cyber security ecosystem. New Brunswick, for instance, was the first province in Canada to develop a comprehensive strategy on cyber security and cyber innovation. The main thrust of the New Brunswick's cyber security action plan is to build cyber security capacity and expertise through academic programs and developing partnerships with the private sector.[23]

To strengthen R&D in cyber security, some of the interviewees highlighted the need for the Government of Canada to increase its investment in this area. Although most of the suggestions that were made may go beyond the Strategy's original design, these suggestions are provided here in the spirit of lessons learned and for the purpose of future planning. According to these interviewees, there is an opportunity for the Government of Canada to further invest in:

- a comprehensive strategy to assure development of the required skillsets and recruitment and retention of highly valued cyber security workforce;
- cyber security start-up companies to take root in Canada;
- Canadians and Canadian companies to develop entrepreneurship in cyber security; and
- Canadian universities and other educational institutions to offer more courses and programs to cyber security.

3.2 Performance—Implementation

Under this section, the evaluation examined the extent to which the Strategy-funded activities were implemented. If an activity was not fully implemented, the evaluation sought to identify why it was not. The extent to which these activities contributed to the achievement of the Strategy's objectives is illustrated in the next section.

Evaluation Finding: Most of the Strategy-funded activities were fully implemented as intended. Exceptions were DND's Defence Research and Development Canada's activity to develop enterprise architecture and its related deliverables, the RCMP's activity to publish an annual report on cybercrime and Shared Services Canada's activities to secure a Third Internet Connection, as well as to establish a Cyber Infrastructure Recall System.

The participating organizations received funding to deliver specific cyber security related activities. Based on performance information provided, the majority of the Strategy funded activities were implemented as intended. However, the evaluation identified at least four activities that were not fully implemented:

[23] http://cybernb.ca/en/news/.

- DND's Defence Research and Development Canada was to design and implement an enterprise architecture framework, as well as a common Cyber Security Lexicon and Taxonomy Document. Defence Research and Development Canada reported that on April 12, 2011, its representatives presented an architecture work plan, an approved Project Charter and other documents to the DG Cyber Committee; however, it was not immediately clear as to why the proposal did not proceed. As a result, Defence Research and Development Canada stopped working on the project and directed the $200,000 per year in associated funding to other cyber security related activities.
- The RCMP was to create a Cyber Crime Fusion Centre and publish an annual report on cybercrime and draft a Cybercrime Strategy. A Fusion Centre was created and the RCMP published a report in 2014 covering cybercrime trends from 2010-2013. The Cyber Crime Fusion Centre contributed to criminal intelligence briefs for the law enforcement community and reports produced by the 5-Eyes Cybercrime Working Group.[24] Internal documents reviewed indicated that in fall 2014, the RCMP's Cyber-Crime Fusion Centre resources were moved from Technical Operations to the National Intelligence Coordination Centre;[25] and in December 2015, the RCMP launched its Cybercrime Strategy, which is expected to enable the Force to better combat cybercrime in concert with its domestic and international law enforcement partners and other stakeholders.
- Shared Services Canada was to secure a Third Internet Connection to ensure business continuity of Internet services for Government of Canada and to improve the performance of the existing secure network environment. Shared Services reported that the existing Internet connections were strengthened with higher availability and security controls with all readiness to enable the Third connection with the procured service provider. This Third connection is in the process of being completed.
- Shared Services Canada was also to establish a Cyber Infrastructure Recall System to assure Shared Services' access to information about the IT equipment supporting infrastructure services for its 43 partner departments, supplemented by vulnerabilities and threats related to such equipment and enabling a timely assessment of the impact of compromise. Shared Services established a Supply Chain Integrity Program in collaboration with Communications Security Establishment to proactively address risks associated with the procurement of vulnerable IT hardware, software and services, as well as to address compromised equipment already in service. As part of the Supply Chain Integrity Program, the Communications Security Establishment conducts risk assessments and provides mitigation advice to increase the security posture of new equipment in the Government of Canada network. Based on that guidance, Shared Services takes the business decision to apply appropriate measures to reduce the risks to acceptable levels. As of this writing, Shared Services Canada has conducted more than 21,000 supply chain integrity assessments.

[24] This Working Group consists of representatives from Canada, Australia, New Zealand, the United Kingdom, and the United States.

[25] RCMP reported that, in line with the advancing the second phase of Canada's Cyber Security Strategy, the RCMP resources conducted operational criminal intelligence rather than public reports of cybercrime trends.

As indicated above, a number of organizations reported having difficulty staffing certain technical positions, particularly in a secret and top secret environment.

Three organizations reported under-spending: the Department of Justice spent 90% of the allocated funding; the RCMP and Shared Services reported spending 69% and 85% of allocated funding respectively.[26] Canadian Security Intelligence Services reported that the funding received was to augment its existing work. As such, it was not possible to distinguish exactly what activities occurred based on the funding received. Treasury Board of Canada Secretariat and Global Affairs Canada spent their allocated funding fully. Communications Security Establishment and Public Safety reported spending slightly more than the allocated funding.

The Strategy put in place a horizontal performance measurement framework and produced a progress report that covered horizontal activities over 2012-13 and 2013-14. Although the progress report mentioned the integration of the RCMP's Cyber Crime Fusion Centre's resources into the RCMP National Intelligence Coordination Centre and the publication of the RCMP's inaugural report on cybercrime, it did not address any of the other above-mentioned implementation related issues (i.e., why certain activities had not been implemented as intended).

The difficulty faced by some of the participating organizations in providing relevant performance information may indicate that such information was not being collected regularly and consistently and/or readily available.

Given that the oversight committees did not keep meeting minutes, and in the absence of any other documentation, the evaluation was unable to determine the process that was used by individual organizations or collectively in deciding not to fully implement the Strategy funded activities. It was also unable to establish the extent to which the oversight committees were informed about these developments. As such, the evaluation considers the partial implementation of certain Strategy funded activities as a deviation from the Strategy's original design.

Observations and Opportunities for Improvement

The issues raised above underline the need to strengthen the Strategy's Performance Measurement Framework to collect performance information that is relevant, reliable and outcome oriented on a regular and consistent basis, as well as to track program expenditures. Such performance expenditure-related information should be provided to the oversight committees so that they can fulfill their responsibilities in monitoring the progress made by the participating organizations on the implementation of the Strategy and improving the Strategy's performance on an ongoing basis.

[26] Subsequent to its creation, Shared Services assumed responsibility for 43 partner organizations' existing security postures at varying levels of maturity. Shared Services Canada reported that in 2014-15, it formalized a cyber and IT security program, which was followed by the creation of a dedicated Branch in 2015-16. Subsequently, Shared Services significantly increased the proportion of its own appropriation on cyber security expenditures to deliver cyber and IT security services related to the strategic objectives of the Strategy.

3.3 Performance—Effectiveness

This section addresses issues such as the extent to which the Government of Canada has secured its systems and strengthened its capacity to prevent cyber incidents and detect and defend against cyber threats. The section also considers how well the Government of Canada has responded to and recovered from cyber incidents. In addition, the section examines progress in establishing partnerships to secure vital cyber systems outside the Government of Canada, as well as in helping Canadians to be safe online. The latter will be addressed through an examination of the success of public awareness campaigns in enhancing Canadians' knowledge of online threats, and the extent of law enforcement agencies' awareness of cybercrime trends.

3.3.1 Progress in Securing the Government of Canada's Systems

Evaluation Finding: The Government of Canada has increased its capacity to prevent, detect, respond to, and recover from cyber attacks. This increase is evidenced by a steady decline in data breaches and an improved ability of the government organizations to quickly analyze and contain breaches. These accomplishments exist despite an increase in state- and non-state-sponsored cyber attacks against Government of Canada networks in recent years.

All interviewees agreed that the Government of Canada has increased its capacity to prevent, detect, respond to, and recover from cyber incidents. The Government's investment in Canada's Cyber Security Strategy was argued to have directly contributed to these achievements. Accordingly, in 2009 and before the establishment of the Strategy:

- the approach to cyber security was extremely fragmented;
- there was little capacity to detect and/or prevent cyber threats;
- Government organizations had different IT security infrastructure, security postures and maturity levels, and had assumed differing levels of risk;
- the cyber security roles and responsibilities of government organizations were unclear, and these organizations were, for the most part, on their own to protect their systems;
- many obstacles impeded information sharing; and
- the Government of Canada IT system suffered from many vulnerabilities. These vulnerabilities included more than 2900 Internet access points and more than 400 data centres, which provided ample opportunities to exploit or disrupt the Government of Canada systems.

Following the advent of the Strategy and the implementation of subsequent cyber security initiatives, such as the creation of Shared Services Canada, the Canadian Government's IT infrastructure was consolidated, centralized and improved. This consolidation resulted in Shared Services Canada developing and implementing an enterprise approach for the delivery of IT security services to its customers. For example, the number of Internet access points was reduced to two core enterprise Internet services (with a Third under construction); three enterprise data centres were established; and a process was started to consolidate email systems down to one, which is still underway.

In addition to security benefits inherent in this consolidation, such as reducing the "attack surface," for the first time, an enterprise-wide approach to cyber security was developed for the Government of Canada. The approach included establishing a close working relationship amongst lead security agencies by putting in place a tripartite governance structure with a specific focus on protecting and securing Government of Canada systems.[27]

This approach and the implementation of the following measures have resulted in improving the Government's ability to prevent, detect and manage IT threats:[28]

- A single enterprise-wide, 24/7/365 Security Operations Centre to monitor, detect and respond to cyber events was established within Shared Services Canada and a Government of Canada wide incident management process was promulgated by Treasury Board of Canada Secretariat in collaboration with Shared Services Canada. To date the Security Operations Centre has triaged over thousands of cyber events and managed related confirmed cyber incidents. At the current rate, incident investigations are projected to increase 261%[29] due to the continuous improvements in monitoring and detection.
- A specialized and mobile Cyber Recovery team was created at Shared Services Canada to assure rapid restoration of services following a compromise on Government of Canada IT infrastructure. This includes forensics services to investigate cyber events and their causes, in order to implement future mitigations. The recovery team was deployed coast to coast to coast, worked closely with at least 25 different departments and agencies to provide assistance, guidance and leadership on a high number of documented incidents. Based on observed trends between 2014-15 and 2015-16, all activities related to forensics are projected to increase as follows: 137% in forensic investigations and recovery, 240% in Shared Services Canada forensics investigation assistance to Departmental Security Officers, and 144% in advice and guidance.
- Deployment of advanced detection and deterrence capabilities to a significant number of departments. In 2016, the number of attempts to identify and exploit vulnerabilities in Government of Canada networks and systems that CSE blocks on a daily basis increased almost tenfold. Consolidation of Government of Canada networks has enabled the government to deploy these detection and deterrence capabilities simultaneously. Accordingly, should a vulnerability be detected at a single department, it can serve as an early warning for protection of all departments on the consolidated network. Based on the current threat surface, network level defences are not enough, and should be complemented by end point protection.
- A comprehensive Supply Chain Integrity Program to assure only trusted IT products (hardware, software) and services are acquired and implemented and that mechanisms are in place to mitigate compromised equipment in a timely manner. To date, the program has completed over 16,000 supply chain integrity reviews, with the 2015-16 statistics, representing a 300% increase from the previous year.

---

[27] Security Tripartite Committees includes representatives from Communications Security Establishment, Treasury Board of Canada Secretariat, and Shared Services Canada at DG, ADM and DM levels.

[28] Progress to date is as of April 1, 2016.

[29] 2015-16: 1163; 2016-17 – first 5 months: 1197.

- Geographically dispersed redundant IT infrastructure to ensure the availability of systems in the event of a cyber-incident; augmented security and resiliency of two core Internet service access points and upgraded infrastructure to accommodate a Third Internet connection in a distinct geographical location for additional robustness. Implementation of an *interim* hot (live[30]) alternate Security Operations Centre in a distinct geographical location.
- A plan has been implemented for managing Government of Canada level cyber security events. Since its inception in December 2015, the plan and its associated processes and procedures have been used on numerous occasions to guide Government of Canada cyber security stakeholders (including TBS, SSC and CSE) in handling threats to, and vulnerabilities within, government systems, and has served as a template for providing support to departments that are coordinating events of national importance (such as the 2016 federal election).
- An Assistant Deputy Minister level cyber security event management exercise was conducted to ensure executive level understanding of Government of Canada cyber security event management processes. The EnGarde 2016 exercise brought together representatives from 13 departments to familiarize senior leaders on cyber security roles and responsibilities, information flow and collaboration requirements, and strategic communications processes and protocols.
- An Enterprise Security Architecture (ESA) program has been implemented to provide a standardized approach to the development of Government of Canada IT security architectures thereby ensuring that basic security building blocks are implemented across the enterprise as the Government's infrastructure is being renewed. The ESA program has provided detailed tools and templates for use by departments and agencies in integrating security into their IT programs. In particular, ESA has been used to successfully implement a security by design approach for Shared Services Canada's transformation initiatives such as the Electronic Transformation Initiative, Back Office Transformation projects including GCDOCS,[31] My GCHR,[32] and the Government of Canada Interoperability Platform, and the Government of Canada Cloud Adoption Strategy.
- The Government of Canada IT Strategic Plan, in which security is a key driver, was published in 2016. Covering the five year period of 2016–2020, the plan articulates the need for layered defences to reduce exposure to cyber threats, use of trusted IT to ensure secure processing and storage of data and information, and increased threat awareness and understanding. The plan also outlines a variety of ongoing and future initiatives that will be implemented enterprise-wide to evolve the Government of Canada's cyber security posture.

---

[30] According to Shared Services Canada, the requirement was to implement an alternate cold standby site; however, the Agency implemented a live site using A-Base funding to assure the seamless continuity of this critical service.

[31] GCDOCS is an Electronic Document and Records Management Solution that is being deployed as part of the Government of Canada's Open Government Initiative to allow for consistent record keeping.

[32] My Government of Canada HR (MyGCHR) supports departments as they transition from their existing departmental HR applications to a single instance of Government of Canada standard.

The Strategy funded activities have contributed to this increase in government's capacity to prevent, detect, respond to, and recover from cyber incidents. CSE, for example, has increased its capacity to defend Government of Canada's networks and systems by deploying cyber defence services in cooperation with Shared Services Canada. As such, CSE defends the majority of government departments and agencies from cyber threats. To do so, CSE analyses tens of terabytes of network and system telemetry and performs hundreds of millions of direct defensive mitigations on Government of Canada networks and systems every day.

Many interviewees indicated that without the improved protection offered by Canada's Cyber Security Strategy, given the evolution and sophistication of threats today, the Government of Canada cyber systems would have been constantly disrupted.

Although cyber incidents and breaches still happen, they are becoming less frequent.

- Based on performance information provided by CSE, the Government of Canada blocks on average more than 600 million attempts each day to identify or exploit vulnerabilities in its systems and networks.
- According to the same source, between 2013 and 2015, the Government of Canada detected, on average a year, more than 2500 state-sponsored cyber activities against its networks.

Although more than six percent of these attempts breached the Government of Canada's systems in 2013, this number had fallen to less than two percent in 2015.

Some interviewees felt that a breach rate of even two percent is unacceptable and that there should be zero tolerance for such breaches. However, the majority of interviewees indicated that preventing all cyber attacks is unrealistic. These interviewees argued that the Government of Canada should focus on reducing the risk of attacks and minimizing their impacts.

Canada's Cyber Security Strategy has equipped the Government of Canada to respond more quickly to cyber intrusions and to recover from them faster. The Government has put in place a Cyber Security Event Management Plan based on lessons learned from previous attacks. As well, the Government has adopted a better disaster recovery regime, including allowing a single entity to control the recovery process, which had not been possible in the past.

These steps have also helped improve the recovery process. Due to the comprehensive scope of Government of Canada Cyber Defence programs, the cost and time of compromises has been reduced significantly. For example, a compromise in 2014, before these measures were put in place, cost tens of millions of dollars and months to address; with these defences in place, a similar attempted compromise was addressed in less than a week at minimal cost.

Canada Revenue Agency's recovery from a security bug called "Heartbleed" in 2014 was identified as a good example of how to respond to and recover from a cyber-attack. Canada Revenue Agency acknowledged the breach immediately and quickly brought in experts to contain its impact.

Observations and Opportunities for Improvement

Despite its many cyber security advances, deficiencies remain. Many interviewees observed that the Government of Canada needs to further strengthen its capacity to prevent, detect, respond to, and recover from cyber attacks through:

- better engagement with international actors to develop international norms to reduce cyber threats (i.e., developing a cyber foreign policy);
- development of an enterprise Government of Canada security information and event monitoring toolset (the foundation of security monitoring and detection), and an enterprise Government of Canada development, testing and integration lab;
- dynamic investment in capital for classified infrastructure to support secure department to department information sharing and processing (currently, classified communications equipment is funded on a partner cost-recovery basis – infrastructure investment is required upfront to put the dedicated infrastructure in place); and
- broader implementation of mitigation measures developed by the Communications Security Establishment was argued by some of the interviewees would eliminate the vast majority of cyber threats to the Government of Canada's systems.[33]

3.3.2 Progress in Securing Systems of Importance to Canada

Evaluation Finding: The Strategy has helped forge partnerships with critical infrastructure owners and operators and other private sector stakeholders. However, according to some of the interviewees and literature reviewed, the overall progress to secure systems of importance to Canada (i.e., vital infrastructure) has been limited.

Numerous sector-specific and cross-sector fora, tables, and advisory groups were created to engage with officials from provincial and territorial governments, critical infrastructure owners and operators, and other private sector stakeholders on cyber security issues.

Since the Strategy's launch, several hundred engagement activities were held with the critical infrastructure sectors, including other levels of government. Similarly, critical infrastructure owners and operators and other private sector stakeholders attended numerous Strategy

[33] In 2014, CSE recommended that Government of Canada organizations implement CSE's top 10 mitigation measures to improve network security. This list included using Shared Service Canada's (SSC's) internet gateways. CSE believed that users would subsequently benefit from "the protection provided by higher level cyber defences deployed at the enterprise level that monitors for, and can respond to, unauthorized entry, data exfiltration or other malicious activity" (https://www.cse-cst.gc.ca/en/node/1297/html/25231). The Office of the Comptroller General's *2015 Horizontal Internal Audit of Information Technology Security in Large and Small Departments* found that "these control frameworks were not implemented in most departments as well as on the IT infrastructure." Some of the interviewees in our evaluation indicated that the infiltration of the National Research Council's (NRC's) networks in 2014 could be directly attributed to NRC's choice not to use SSC's gateways and to remain outside the Government of Canada standard networks. According to media reports, the NRC infiltration shut down the NRC's systems for several months and necessitated a year-long IT overhaul at an estimated cost of $32.5 million (http://ottawacitizen.com/news/politics/cyber-attack-at-nrc-kept-secret-from-other-departments).

sponsored training and awareness sessions. In addition, CSE cyber security architects, among other things, provided advice and guidance to mitigate supply chain risk and collaboratively develop best practices for specific sectors.

CSE implemented the Enhanced Technology and Information Sharing program to share CSE's threat intelligence and cyber defence capabilities with Canada's private industry and critical infrastructure sectors through a series of on-going initiatives. CSE has active relationships with several partners from across Canada's critical infrastructure sectors, including the finance industry, telecommunications providers, and managed security services. CSE has developed a series of storyboards detailing the capabilities and services that it intends to deploy to help defend Canadian critical infrastructure partners. Three of those storyboards have evolved to the project phase.

As part of enhancing the cyber security of Canada's critical infrastructure, CSE is working with various Canadian financial institutions to combat financial cyber fraud and to share compromised credit card numbers and indicators of compromise exploited through a malware targeting Point-of-Sale terminals.

CSE and Public Safety represent the Government of Canada on the Canadian Cyber Threat Exchange (CCTX) Board of Directors in an advisory role. CCTX is a private-sector led, national cyber security information sharing organization, represented by the major sectors of critical infrastructure, which provides a single point of contact for private sector collaboration on cyber security.

The Canadian Cyber Incident Response Centre expanded its operations and increased its technical capabilities (both preventative and reactive), including its ability to collect and analyze information. There are at least 1300 private sector organizations that receive the Canadian Cyber Incident Response Centre's alerts on a regular basis.

Today, the Government of Canada engages with critical infrastructure owners and operators and other private sector stakeholders substantially more than it ever has. The majority of the interviewees have attributed this level of engagement and outreach activities directly to the Strategy and its investment in this area. These and other Public Safety led outreach activities provided educational opportunities, as well as a good national and international presence.

Observations and Opportunities for Improvement

Notwithstanding these improvements, certain deficiencies have also been identified.

- The Strategy's overall investment in securing systems of importance to Canadians was described by some of the interviewees to be inadequate. Interviewees pointed out that the majority of government's investment has been on securing its systems.
- Roles and responsibilities need to be clearer, particularly those of CSE and the Canadian Cyber Incident Response Centre. Specifically, there is a need to clarify which organization should serve as the first point of contact for the private sector in the event of a cyber-incident.

- Limited progress has been made in both establishing reciprocal norms for sharing information and forging partnerships with the private sector, as well as with provinces and territories.
- Private sector companies seem to lack trust in the public sector's ability to safeguard their information.
- There is no clear policy on how to engage with companies that hold sensitive government information but are not critical infrastructure owners and operators.

3.3.3 Progress in Helping Canadians to be Secure Online

Evaluation Finding: There is a perception among the majority of the interviewees that Canadians are more aware of cyber threats today than they have been in years past. However, this increased awareness does not necessarily mean that "Canadians are safer online" or be attributed to Public Safety's public awareness campaign.

The Public Awareness Campaign: Public Safety Communications coordinated cyber security public awareness and communications activities, including advertising, social marketing, partnerships, web media relations, exhibits, and special events.

Shortly before the launch of the Public Awareness Campaign, Public Safety conducted public opinion research to gauge Canadians' knowledge, attitudes and behaviours towards cyber security. This research was intended to be conducted on an annual basis to measure progress.

The research concluded that there was a general expectation that "an awareness campaign should deliver simple, straightforward and action-oriented information that is within the means of Canadians to carry out."

To this end, and in an attempt to reach a wide audience, the department undertook a range of activities, from placing paid radio and online ads to establishing paid and unpaid partnerships. These partnerships involved public sector organizations and various media outlets, retailers, and other private sector organizations including Bell, TELUS, Best Buy, Twitter, Facebook, and LinkedIn. The Department also:

- launched the Get Cyber Safe website and its French equivalent (Pensez cybersécurité); these websites provide simple steps that Canadians can take to protect themselves online;
- partnered with STOP. THINK. CONNECT, a global cyber security awareness partnership; the partnership comprises a coalition of private sector companies and non-profit and government organizations, including the US Department of Homeland Security;
- developed toolkits and guides for small and medium size businesses, as well as the finance, banking, and telecommunications sectors; and
- launched the Cyber Security Awareness Month, which is observed every October to help Canadians learn how to stay safe online.

Through these activities, hundreds of hours of promotional and educational programming was produced.

The public awareness campaign generated a significant number of output-related statistics (e.g., the number of people who visited a website or attended an educational event). Nonetheless, no information was available to conclude to what extent these activities contributed to the intended Strategy outcome that "Canadians are safe and secure online."

Contrary to the original plan, Public Safety Communications as a result of Government's decision to consolidate the number of public opinion surveys, was unable to annually survey public opinion to measure progress on reaching the benchmarks established in the baseline public opinion research. Relying on information from interviews and a literature review, the evaluation was unable to determine to what extent the public awareness campaign increased awareness or changed behaviour.

Law Enforcement Agencies' Awareness of Cybercrime Trends: The RCMP was to create a Cyber Crime Fusion Centre to advance situational awareness and analysis of cybercrime trends and to draft a Cybercrime Strategy. The Centre was intended to:

- address key analytical cybercrime gaps;
- better assess and help respond to criminal cyber incidents;
- provide a more comprehensive understanding of cybercrime threats and risks; and
- publish an annual report on cybercrime and describe the work done on collecting and analyzing statistics.

According to documents reviewed and the RCMP officials interviewed as part of this evaluation, the RCMP created a Cyber Crime Fusion Centre in 2011, which provided law enforcement with information to support a more comprehensive understanding of the cybercrime threats and risk environment.

In 2014, the RCMP published a report entitled *Cybercrime: An Overview of Incidents and Issues in Canada*.[34] The report covered cybercrime threats and trends, provided a formal definition of the various types of cybercrime, presented statistics on the nature and extent of reported cyber incidents in 2011 and 2012 and covered examples and case studies from 2010, 2011, 2012 and 2013.

Although the inception documents specify that the Cyber Crime Fusion Centre would produce an annual RCMP report on cybercrime, RCMP reported that, in line with the advancing the second phase of Canada's Cyber Security Strategy in 2014, the RCMP resources conducted operational criminal intelligence rather than public reports of cybercrime trends.

In 2015, the RCMP launched its Cybercrime Strategy which aims to reduce the threat, impact and victimization of cybercrime in Canada through law enforcement action.

Cybercrime Policy and Legislative Development: The Department of Justice was responsible to provide legal advice, support partnerships by representing Canada at international and federal/provincial/ territorial fora, and develop cybercrime policy and legislation.

[34] http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada.

The Criminal Law Policy Section of the Department of Justice engaged in a number of activities, including the provision of legal advice. It has participated, among other things, in discussions of cybercrime at the United Nations, in the criminal law context, at the Council of Europe, in relation to the *Convention on Cybercrime*, which is in force in Canada.

The Department was also involved in developing cybercrime policy and legislation, including recent amendments to the *Criminal Code*, the *Competition Act*, the *Canada Evidence Act* and the *Mutual Legal Assistance in Criminal Matters Act* (former Bill C-13) and the amendments to the *Criminal Code* in the *Anti-Terrorism Act* (former Bill C-51) as well as the amendments to the *Criminal Code* to ensure the constitutionality of section 184.4 (former Bill C-55).

The imposition of certain government-wide and departmental spending limitations, particularly on travel, negatively impacted the Department of Justice's ability to represent Canada at international and federal/provincial/territorial fora.

Observations and Opportunities for Improvement

Many interviewees said that they were unfamiliar with the public awareness campaign, and therefore, declined to comment on this initiative. This lack of familiarity perhaps underlines the need to increase the campaign's visibility.

Some interviewees who did comment on the campaign highlighted the need to incorporate cyber security into school curriculums.[35] This need was also raised in Toronto by participants at the March 2016 Public Policy Forum on Securing Canada's Cyberspace. Participants recommended that "elementary, secondary and post-secondary schools could do more to teach students about cyber security and online etiquette." The Forum also recommended that "Education programs must also seek to inform and educate parents, many of whom do not understand how cyber threats can impact their families."[36]

There is a need to conduct follow-up surveys to gauge Canadians' level of cyber security awareness and to measure progress on reaching the benchmarks established in the baseline public opinion research. These surveys can also inform future campaign planning.

There appear to be low levels of cybercrime reporting to police. Canadians are faced with myriad ways to report these crimes to police and governments, which causes confusion. Businesses appear to be reluctant to report these crimes because of how it may adversely affect their revenue or reputation—or both. [37]

[35] Note that this does not fall under federal government's direct jurisdiction.
[36] http://www.ppforum.ca/sites/default/files/Securing%20Canada%27s%20Cyberspace%20-%20Toronto%20report%20-%20Final_0.pdf, page 10.
[37] https://www.thestar.com/business/2015/08/19/canadian-companies-have-no-incentive-to-report-cyber-attacks-like-that-on-ashley-madison.html.

Based on the most recent data available from Statistics Canada, in 2013, "more than half of all cybercrime reported [to police] was described as a fraud violation, with 6,203 offences out of a total of 11,124 offences across all categories."[38]

4. EVALUATION FINDINGS AND CONCLUSIONS

The governance structure of Canada's Cyber Security Strategy has helped participating organizations share information, collaborate, and coordinate with one another. However, in the absence of supporting documentation, the evaluation was unable to assess the governance structure's overall effectiveness.

With the exception of the DG Cyber Operations Committee, none of the cyber oversight committees has met regularly and none of the oversight committees maintained meeting minutes on a consistent basis. This inconsistency in record keeping limited the evaluation's ability to verify the extent to which the oversight committees fulfilled their roles and responsibilities as outlined in their terms of references, including monitoring the Strategy's implementation and progress on ongoing basis.

While the Strategy has helped clarify the roles and responsibilities of participating organizations, the evaluation has identified specific instances where there was a perception of overlap in the roles and responsibilities. This has caused confusion and frustration for the departments and agencies involved, as well as their private sector stakeholders.

This confusion applies particularly to the roles and responsibilities of the Canadian Cyber Incident Response Centre and CSE. Many interviewees told us that, based on their interactions, the private sector is unclear who in the government to contact first in the case of an incident or any other cyber-related issues.

Participating organizations share information, for the most part, on an ad hoc and selective basis. No clear policy states what information should be shared with whom and when. The organizations typically decide on their own terms what to share with others. As well, the organizations have no efficient way of sharing classified information, particularly in real time.

Most of the Strategy-funded activities have been implemented as intended. The evaluation identified four instances where the funded activities were not implemented fully. Three organizations have reported under-spending of the allocated funding and two organizations did not or were unable to track their relevant expenditures. In addition, three organizations have indicated having difficulty staffing certain technical positions particularly in a secret and/or top secret environment.

The Strategy has helped forge partnerships with critical infrastructure owners and operators and other private sector stakeholders. However, according to the interviewees, progress to secure systems of importance to Canada (i.e., vital infrastructure) has been limited. The Strategy's overall investment in securing systems of importance to Canada was described as inadequate,

[38] http://www.statcan.gc.ca/daily-quotidien/150609/dq150609d-eng.pdf.

and there has been limited progress made in establishing reciprocal norms for sharing information and forging partnerships with the private sector, as well as with provinces and territories.

The Government of Canada has increased its capacity to prevent, detect, respond to, and recover from cyber attacks. The number of data breaches has steadily declined, and the Government can now analyze and contain breaches more quickly than had been possible in the past. These improvements exist despite an increase in state- and non-state-sponsored cyber activities against Government of Canada networks in recent years.

Although Public Safety has undertaken many activities to make Canadians aware of cyber security, it is unclear to what extent these activities have made Canadians safer online.

Given these findings, the evaluation has identified a number of opportunities for improvement and has put forward several recommendations to address them. However, as indicated elsewhere in this report, the Government of Canada has undertaken, through a parallel process (i.e., Ministerial Mandate Letter), a comprehensive review of existing measures to protect Canadians and Canada's critical infrastructure from cyber threats. It is anticipated that this process will result in overhauling Canada's Cyber Security Strategy that was the subject of this evaluation and will establish a new and more comprehensive approach to address cyber security related issues, including those that have been identified in this evaluation.

Regardless of what may replace the current Strategy, from a program design and program evaluation perspective, key challenges facing participating organizations going forward will be to sustain the achievements to date, while continuing to strengthen horizontal governance, accountability and performance monitoring to ensure that Canada is better prepared to maintain its security posture in an era of constantly evolving and increasingly complex cyber threats. It is in this context that the following recommendations are being made for consideration.

5. RECOMMENDATIONS

In collaboration with participating organizations, the Senior ADM of the National and Cyber Security Branch, Public Safety, should consider undertaking the following:

1) Strengthen horizontal governance of cyber security in the Government of Canada by:

    a) re-assessing the governance structure to determine the need and demand for the current committee configuration and to improve participation;

    b) improving the provision of secretariat support, including coordination, information management and other administrative services;

    c) ensuring that governance committees have terms of references that clearly define roles, responsibilities, and expectations from members;

    d) ensuring that the oversight committees fulfill their roles and responsibilities as outlined in each oversight committee's terms of reference; and

e) keeping meeting minutes on a consistent basis.

2) Strengthen the Cyber Security related information-sharing practices by developing clear policies, procedures and tools to ensure timely and systematic exchange of information among partners and stakeholders.

3) Strengthen the Strategy's performance measurement and data collection practices by:

   a) collecting relevant, reliable and outcome oriented performance information, including information on program expenditures, on a regular and consistent basis; and

   b) providing performance and expenditure information collected to the appropriate oversight committees on a regular basis to support effective monitoring and accountability.

6. MANAGEMENT RESPONSE AND ACTION PLAN

In parallel with this evaluation, Public Safety Canada has been leading a comprehensive review of cyber security, which is intended to result in a renewed cyber security strategy for the Government of Canada. The evaluation recommendations will inform the development of the renewed approach with respect to:

- Cyber security governance;
- Information sharing within the federal government and with external partners; and
- Performance measurement and data collection practices.

Recommendation	Management Response	Action Planned	Planned Completion Date
1. In collaboration with participating organizations, the Senior ADM of the National and Cyber Security Branch, Public Safety, should consider undertaking the following: Strengthen horizontal governance of cyber security in the Government of Canada by: a) re-assessing the governance structure to determine the need and demand for the current committee configuration and to improve participation; b) improving the provision of secretariat support, including	Accept	Through the policy renewal process following the completion of the Government of Canada Cyber Review: a) Consider options to enhance the effectiveness of cyber security governance mechanisms within the federal government, including committee configuration and membership. b) Explore options for formalizing support to internal governance mechanisms, with special attention paid to formalizing communications and information management practices. c) Revisit existing terms of reference	October 2018

coordination, information management and other administrative services; c) ensuring that governance committees have terms of references that clearly define roles, responsibilities, and expectations from members; d) ensuring that the oversight committees fulfill their roles and responsibilities as outlined in each oversight committee's terms of reference; and e) keeping meeting minutes on a consistent basis.		for cyber committees and adapt as necessary to ensure that roles, responsibilities and expectations from participants are clear. d) Explore measures to improve accountability in federal governance of cyber security. e) Assess record-keeping options for any governance mechanisms (e.g. formalized minutes, records of decision).	
2. Strengthen the Cyber Security related information-sharing practices by developing clear policies, procedures and tools to ensure timely and systematic exchange of information among partners and stakeholders.	Accept	Explore options (policies, procedures, tools) for improving information sharing practices with partners (within the federal government) and stakeholders (between the Government and external partners).	December 2017
3. Strengthen the Strategy's performance measurement and data collection practices by: a) collecting relevant, reliable and outcome oriented performance information, including information on program expenditures, on a regular and consistent basis; b) providing performance and expenditure information collected to the appropriate oversight committees on a regular basis to support effective monitoring and accountability.	Accept	Update the horizontal performance measurement strategy to reflect the priorities of a renewed cyber security strategy. a) Ensure that outcomes identified in the updated performance measurement strategy are attainable and measurable, and that performance indicators are relevant. b) Ensure that implementation of the performance measurement strategy includes periodic reporting to an oversight body (e.g. cyber security committee or comparable mechanism)	October 2018

ANNEX A: ROLES AND RESPONSIBILITIES[39]

Department	Role and Responsibilities		
	Pillar 1	**Pillar 2**	**Pillar 3**
PS	Lead and coordinate the implementation of the Strategy, including the design of the overall approach to performance measurement and reporting for the Strategy.	-Lead and coordinate the engagement with provinces and territories, the private sector, the Government of Canada, and international stakeholders. -Build linkages to Canada's cyber security academic experts.	Lead and coordinate public awareness activities to inform Canadians of the risks they face and the actions they can take to protect themselves and their families in cyberspace.
CSE	-Monitor and defend Government of Canada networks by detecting, discovering, and responding to sophisticated cyber threats to the Government and provide mitigation and recovery advice and guidance to Government departments to help them recover from cyber incidents. -Collect, analyze, and report on foreign intelligence and serve as Canada's interface with the Five-Eyes cryptologic community. -Undertake classified cyber security research and development. -Provide technical expertise and advice on architecture design and the proper selection and use of IT security products.	-Engage, coordinate and exchange information to enhance national and international collaboration on cyber security. -Partner with the private sector to strengthen Canada's cyber resiliency and help secure critical infrastructure of importance to the Government of Canada.	

[39] The information compiled in this table has been taken from a number of documents, including Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, pages 9 to 13 (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf), as well as a document entitled Measuring the Performance of Canada's Cyber Security Strategy, page 11.

Department	Role and Responsibilities		
	Pillar 1	**Pillar 2**	**Pillar 3**
	-Provide IT security training and awareness programs to all Government of Canada IT security professionals and other employees.		
SSC	-As the GC's Computer Incident Response Team (GC-CIRT) protect Government of Canada IT infrastructure by coordinating incident response and producing/ disseminating awareness products. -Protect SSC managed IT infrastructure by monitoring, detecting, discovering, and responding to cyber threats and providing mitigation and recovery advice and guidance to Government departments to help them recover from cyber incidents. -Assure only trusted IT products and services are acquired and deployed on Enterprise IT infrastructure through a comprehensive supply chain integrity program and remediating compromised products that are in-service. -Support the Government of Canada as the enterprise service provider responsible for consolidating and modernizing IT infrastructure to enterprise-class IT products and services that are reliable and secure. -Support Government of Canada cyber security partners in the implementation of horizontal cyber security strategies.		
DND/DRDC	Support cyber security research and development activities:	Support cyber security research and development activities.	

Department	Role and Responsibilities		
	Pillar 1	**Pillar 2**	**Pillar 3**
	• framing the design and implementation of a cyber enterprise architecture framework; • common cyber taxonomy on a common GC Wikipedia (GC pedia) for interoperability; • problem definition statements and analysis of linkages between threats, vulnerabilities, risks and capability gaps; • a report on best practices; • report on new approaches to innovative solutions.		
TBS	Establish and oversee a government-wide approach to cyber security, including: • setting government-wide direction and establishing priorities for securing government IT systems and networks; • providing direction and advice to lead security agencies on the approach and implementation of measures for managing IT security incidents; and • providing oversight to IT incident management, including post-mortem reviews and lessons learned.		
CSIS	-Conduct national security investigations. Report to and advise the Government of Canada on activities constituting a threat to the security of Canada	-Conduct national security investigations. -Report to and advise the Government of Canada on activities constituting a threat to the security of	

Department	Role and Responsibilities		
	Pillar 1	**Pillar 2**	**Pillar 3**
	as defined in the *Canadian Security Intelligence Service Act*. -Assist the Government of Canada to understand cyber threats and the intentions and capabilities of cyber actors in Canada and abroad who pose a threat to Canada's security. This intelligence enables the Government of Canada to improve its situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threats, and take action to secure critical infrastructure.	Canada as defined in the Canadian Security Intelligence Service Act. -Assist the Government of Canada to understand cyber threats and the intentions and capabilities of cyber actors in Canada and abroad who pose a threat to Canada's security. This intelligence enables the Government of Canada to improve its situational awareness, better identify cyber vulnerabilities, prevent cyber espionage or other cyber threats, and take action to secure critical infrastructure. -Liaise directly with the private sector and offer critical infrastructure companies with domain awareness briefings on the topic of advanced persistent cyber threats with the goal of increasing intelligence collection.	
GAC		-Engage on the international dimension of cyber security. -Engage through bilateral and multilateral diplomacy to shape the international policy environment with respect to cyberspace, including through the promotion of the applicability of international law in cyberspace; the promotion of norms for state behaviour in cyberspace; and the development of confidence-building measures to reduce the risk of conflict. -Develop a cyber-foreign policy that will help strengthen coherence in the Government of Canada's engagement abroad on cyber security.	

Department	Role and Responsibilities		
	Pillar 1	**Pillar 2**	**Pillar 3**
		-Assist international partners to protect themselves from cyber threats.	
JUS		-Provide legal advice to all implicated departments in the Government of Canada as required. -Represent Canada at international and federal, provincial, and territorial fora.	
RCMP			-Establish a Cybercrime Fusion Centre to enhance the assessment of criminal cyber incidents and provide law enforcement with a more comprehensive understanding of cybercrime threats and risk environment. -Develop a Cybercrime Strategy to deal with all aspects of cyber criminality, including fraud, organized crime and identity theft. -Publish an annual RCMP report on cybercrime, covering incidents and emerging trends.

ANNEX B: EVALUATION QUESTIONS

Governance
1. To what extent has the horizontal governance structure been effective?
2. Are various partners' roles and responsibilities clearly defined and adhered to?
3. What is the state of collaboration, coordination, and information-sharing among partners?
PERFORMANCE—IMPLEMENTATION
4. To what extent have the funded activities been implemented?
PERFORMANCE—EFFECTIVENESS
5. To what extent has progress been made in securing Government of Canada systems and strengthening the capacity to: a. prevent cyber incidents; b. detect and defend against cyber threats; and c. respond to and recover from cyber incidents?
6. What progress has been made in securing vital cyber systems outside the Government of Canada?
7. What is the state of national and international collaboration on cyber security?
8. To what extent are Canadians more safe and secure online? a. To what extent have public awareness campaigns enhanced Canadians knowledge of online threats? b. To what extent are law enforcement agencies more aware of cybercrime trends? c. What progress has been made in developing cybercrime policy and legislations?
PERFORMANCE—EFFICIENCY AND ECONOMY
9. To what extent has the funding been utilized for the intended purposes?
10. What value has been realized from the investments?
11. Are there alternatives that would provide greater value for money?
12. Are there lessons learned, including from other like-minded countries that could be applied in the Canadian context?