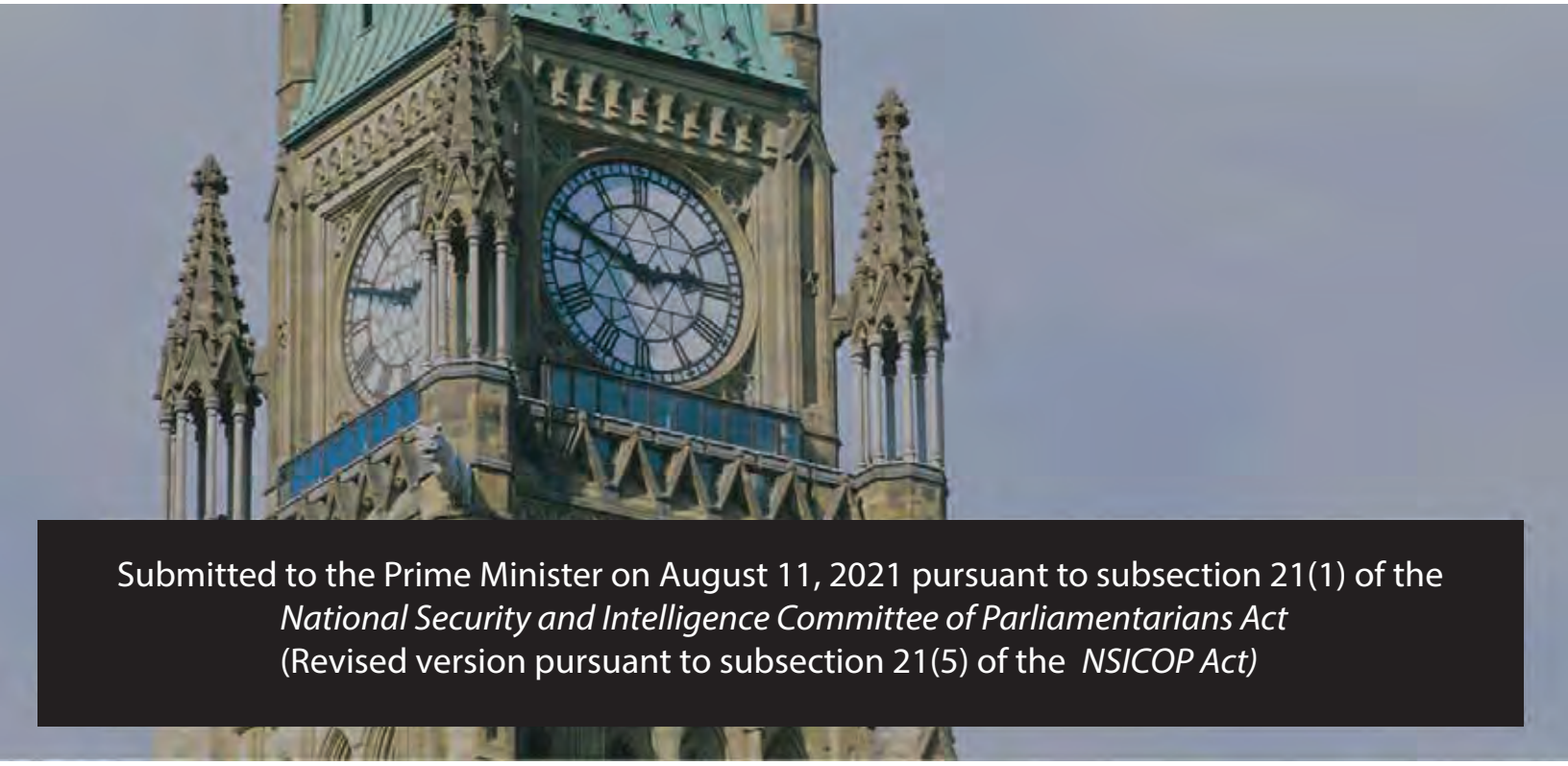
National Security and Intelligence Committee of Parliamentarians

Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack



Submitted to the Prime Minister on August 11, 2021 pursuant to subsection 21(1) of the *National Security and Intelligence Committee of Parliamentarians Act*
(Revised version pursuant to subsection 21(5) of the *NSICOP Act)*

Canada

Ottawa, ON

National Security and Intelligence Committee of Parliamentarians

Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP104-3/2022E (Print)
ISBN 978-0-660-41354-9 (Print)

CP104-3/2022E-PDF (Online)
ISBN 978-0-660-41353-2 (Online)

Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack

The National Security and Intelligence Committee of Parliamentarians

The Honourable David McGuinty, P.C., M.P.
Chair

Submitted to the Prime Minister on August 11, 2021
Revised version tabled in Parliament in February 2022

Revisions

Consistent with subsection 21(2) of the National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), the Committee may submit a special report to the Prime Minister and the ministers concerned on any matter related to its mandate. Consistent with subsection 21(5) of the NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the report that does not contain information the Prime Minister believes the disclosure of which would be injurious to national security, national defence or international relations or is information that is protected by solicitor-client privilege.

This document is a revised version of the Special Report provided to the Prime Minister on 11 August 2021. At the time, the document was classifed as 'Top Secret/Special Intelligence/Canadian Eyes Only.' Revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national security, national defence or international relations or which constitutes solicitor-client privilege. Where information could simply be removed without affecting the readability of the document, the Committee noted the removal with three asterisks (***) in the text of this document. Where information could not simply be removed without affecting the readability of the document, the Committee revised the document to summarize the information that was removed. Those sections are marked with three asterisks at the beginning and the end of the summary, and the summary is enclosed by square brackets (see example below).

EXAMPLE: [*** Revised sections are marked with three asterisks at the beginning and the end of the sentence, and the summary is enclosed by square brackets. ***]

THE NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS

The Hon. David McGuinty, P.C., M.P. (Chair)

Ms. Leona Alleslev, M.P.

Mr. Stéphane Bergeron, M.P.

Mr. Don Davies, M.P.

The Hon. Dennis Dawson, C. P., Senator

Mr. Ted Falk, M.P.
(resigned June 15, 2021)

Mr. Peter Fragiskatos, M.P.

Ms. Iqra Khalid, M.P.

The Hon. Frances Lankin, P.C., C.M., Senator

Mr. Rob Morrison, M.P.

Mr. Glen Motz, M.O.M., M.P.
(resigned June 15, 2021)

Ms. Jennifer O'Connell, M.P.
(resigned March 19, 2021)

Ms. Brenda Shanahan, M.P.

The Hon. Vernon White, C.P., Senator

National Security and Intelligence Committee of Parliamentarians

Chair

Comité des parlementaires sur la sécurité nationale et le renseignement

Président

February 8, 2022

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister and Privy Council
Ottawa, ON
K1A 0A2

Dear Prime Minister:

On behalf of the National Security and Intelligence Committee of Parliamentarians, it is my pleasure to provide you with our Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack. The unanimous report includes four findings and two recommendations to strengthen the government's framework for defending government networks from cyber attack and to extend that framework over federal government organizations as broadly as possible.

Consistent with subsection 21(5) of the *National Security and Intelligence Committee of Parliamentarians Act,* the Special Report was revised to remove information the disclosure of which would be injurious to national security, national defence or international relations, or is information subject to solicitor-client privilege.

Yours sincerely,

The Honourable David McGuinty, P.C., M.P.
Chair
National Security and Intelligence Committee of Parliamentarians

P.O. Box 8015, Station "T" / C.P. 8015, Succursale « T »
Ottawa, Canada K1G 5A6

Table of Contents

Introduction **1**
Overview of the Review **5**
Past Examinations of Cyber Defence Activities **9**
External review 9
The CSE Commissioner 10
Internal review 11
Part I: Cyber Threats – what's at stake and who is involved? **13**
What's at stake? 13
Threats to the personal information of Canadians 13
Threats to business information, intellectual property, research networks and academia 14
Threats to government policies and policy-making 14
Threats to security and intelligence information and operations 15
Threats to the integrity of government systems 15
What's happening? The cyber threat environment 16
Cyber threats to government networks, 2015 to 2020 18
Nation-state advanced persistent threats 22
Government networks and cyber crime 26
Summary 27
Part II: Evolution of the Government's Framework for Cyber Defence **29**
Early days (2001 to 2010) 29
Active network security testing and security posture assessments 30
The origin of computer network defence activities 31
Hard lessons learned along the way 31
Establishing the government enterprise (2010 to 2018) 34
Canada's Cyber Security Strategy, 2010 34
The evolution of Canada's Cyber Security Strategy 38
Part III: Key Cyber Defence Players, Authorities and Activities **41**
Treasury Board of Canada and the Treasury Board of Canada Secretariat 41
Defining government organizations 42
Foundational policies for cyber defence 44
Summary 54

Shared Services Canada 54
SSC mandate 54
SSC services and projects 57
Secure Internet connectivity: The evolution toward the Enterprise Internet Service 61
SSC partners and clients 68
Cyber security event management 70
Summary 71
The Communications Security Establishment 72
CSE cyber-related mandates and authorities 72
Governance of CSE cyber defence activities 76
CSE cyber defence activities 84
Summary 99
Part IV: Governance of Cyber Defence 101
Strategic considerations 101
Operations, policy and programs 103
Incident response 104
Cyber Security Event Management Plan response levels 105
Cyber Security Event Management Plan governance bodies 106
Phases of the cyber security event management process 107
Part V: The Committee's Assessment of the Cyber Defence Framework 111
The evolution of cyber defence in Canada: A virtuous cycle, but incomplete 111
Who is protected depends on who you ask 113
The success and the gap: Securing Internet access in government 114
Crown corporations and government interests 116
Conclusion 119
Findings 121
Recommendations 123
Government response to recommendations 125
Annex A – List of Witnesses 127

Introduction

In early March 2021, governments and organizations around the world became aware of cyber attacks targeting a previously unknown vulnerability in Microsoft Exchange email systems. These attacks were attributed to China, targeted the email communications of victim organizations, and were used to gain persistent access to victim networks. As the attack spread, other sophisticated threat actors quickly took advantage of the vulnerability and hundreds of thousands of organizations were eventually affected. In Canada, the government immediately declared a cyber security event and three organizations – the Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC) and the Canadian Centre for Cyber Security (CCCS) – worked with departments to identify their vulnerabilities and directed them to patch their systems. CCCS also worked to notify hundreds of private sector organizations of their potential vulnerability. Within days, implicated organizations made required changes, and only one government department was affected. As of June 2021, no federal government organizations were found to have suffered any data losses from the attack.[1]

Broadly speaking, the government succeeded in quickly and effectively defending its networks from a serious and previously unknown vulnerability. How did the government come to this point? What challenges remain? Is the government prepared to counter cyber threats in the future? This review seeks to answer these questions.

1. Cyber threats are a significant and pervasive risk to Canada's national security. They affect Canadians at numerous levels, threatening government systems and services, critical infrastructure providers, financial and health systems, research and academic networks, and sensitive personal information. Governments are highly attractive targets for cyber attacks. The federal government holds enormous amounts of data about Canadians, Canadian businesses and innovative sectors such as universities and research institutes. Cyber compromises of this data could reveal sensitive personal information of Canadians and sap the vitality of individual companies and of the economy. The government also manages foreign, trade and security relations through electronic infrastructures that, if compromised, could damage the government's policies and undermine Canada's vital interests. As well, the government provides many critical services, which are heavily dependent on robust and "no fail" electronic infrastructures.

2. Since its inception, the National Security and Intelligence Committee of Parliamentarians (the Committee) has been interested in the security of government systems. Government systems are a core part of Canada's critical infrastructure and integral to national security. Government departments have repeatedly briefed the Committee on the types of cyber threats

[1] Krebs on Security, "At least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software," March 5, 2021, https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/; CSE, "NSICOP Cyber Defence Review. Compromise of Microsoft Exchange," email to NSICOP Secretariat, May 27, 2021; Global Affairs Canada, "Statement on China's Cyber Campaigns," July 19, 2021, https://www.canada.ca/en/global-affairs/news/2021/07/statement-on-chinas-cyber-campaigns.html.

facing Canada, and the Committee summarized those threats in its 2018 annual report to the Prime Minister and then, more thoroughly, in its 2020 annual report. It notes with concern the ubiquity of cyber threats and, in particular, the sophistication and persistence of threats from several foreign states and non-state actors, including the growing threat from ransomware. It also recognizes the significant changes implemented by the government over the last several decades, including updated and new authorities, the creation of new organizations and programs, and major investments in cyber security and defence. In fact, the Committee deferred a review of cyber issues in 2018 to avoid negatively affecting the implementation of recently announced changes to government machinery, notably the creation of the Canadian Centre for Cyber Security and the attendant changes in the roles and responsibilities of Shared Services Canada and Public Safety Canada.

3. Cyber security is a large and complicated field. In the 2018 National Cyber Security Strategy, the government defined it as "the protection of digital information and the infrastructure on which it resides."[2] Such a necessarily broad definition implicates a range of actors in industry, academia and government, and may include everything from procuring hardware, software and services, to developing laws and regulations. Although these areas are potentially critical in their own right, many have little or no relationship with issues of security and intelligence, the core of the Committee's review mandate.

4. The Committee therefore decided to initiate a review of a narrow subset of cyber security activities: cyber defence. Cyber defence may be understood as the technical capability to discover and detect cyber incidents, and to develop and deploy measures to defend against them.[3] In Canada, the Communications Security Establishment (CSE) has been the lead organization in developing and deploying cyber defence activities. Its efforts were facilitated by its complementary role as Canada's signals intelligence organization, which gave it insight into the activities and tactics of the most sophisticated cyber actors, particularly foreign states with the resources and capabilities to mount technically advanced and persistent attacks on target systems and networks (these actors are known as advanced persistent threats). CSE used this insight to build custom cyber defence sensors and defence technologies that could identify and defeat such threats where commercial technologies could not. At the core of CSE's ability to build its operations and adapt them to the rapid evolution of technology has been fundamental changes to statutory authorities. The first major change came in 2001 with the passage of amendments to the *National Defence Act*, which created the authority basis for CSE's information technology security and foreign signals intelligence activities. In 2019, the *Communications Security Establishment Act* came into force, which clarified and expanded those authorities. This report explains that evolution.

5. The framework for cyber defence has two other principal players: Shared Services Canada and Treasury Board, as supported by the Treasury Board of Canada Secretariat. Created in 2011, Shared Services Canada (SSC) plays a mostly operational role. SSC provides

---

[2] Canada, National Cyber Security Strategy, 2018, p. 7.
[3] Canada, Progress Report on the Cyber Security Strategy, undated, p. 9. Original reference is to "network defence."

government departments three key services – networks, email and data centres – and works closely with CSE to address serious cyber incidents. When SSC was created, 43 departments were required to obtain these services from SSC, representing approximately 95 percent of the government's information technology infrastructure spending; the remaining smaller departments and agencies represented the other 5 percent. Those 43 original partners continue to receive all of SSC's services, including those related to cyber security. Over time, 117 other federal organizations have opted to obtain some of these services, bringing the total number of SSC service recipients to 160 out of 169 organizations, totalling 95 percent of all federal organizations.

6. SSC's role in cyber defence is essential in two ways. First, the government has reduced its vulnerability to all forms of cyber attack by consolidating the number of connection points between government networks and the Internet and by reducing the number of legacy data centres. Second, the government has significantly reduced the likelihood of cyber attacks being successful, and the potential damage done if they are, by placing the majority of federal organizations (i.e., those that receive SSC services) behind CSE's sophisticated sensors and cyber defence systems.

7. The Treasury Board and its Secretariat play an overarching role in cyber defence, both as the Chief Information Officer of the government and through directives and policies applicable to all government departments. Treasury Board and its Secretariat have the authority to create policies through various pieces of legislation, most notably the *Financial Administration Act* (FAA). First passed in 1985, the FAA sets out the roles and responsibilities for a number of key actors across government and enables the Treasury Board to issue policies, directives, standards and guidelines for the management and administration of federal entities. Consistent with Canada's parliamentary system, the FAA is a vertical authority structure: individual ministers and their deputies are responsible for the activities of individual departments.

8. Policy instruments promulgated under the FAA are fundamental for cyber defence. They clarify the roles and accountabilities of various departments, providing direction and defining requirements. The most important of these instruments are the Policy on Government Security, the Policy on Service and Digital, the Digital Operations Strategic Plan, the Cloud Adoption Strategy, and the Cyber Security Event Management Plan. They set the framework for cyber security and defence activities. Like all Treasury Board directives, TBS considers the implementation of those related to cyber defence as 'mandatory.' That said, consistent with the vertical authorities in the FAA, deputy heads of individual departments are ultimately responsible for ensuring the integrity and security of their electronic systems and networks and for implementing TBS direction. To address instances of non-compliance, Treasury Board has introduced a compliance management framework, which includes a range of possible administrative consequences.[4]

---

[4] Treasury Board, Framework for the Management of Compliance, 2009. www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=17151.

9. Other authorities play more specific roles in the cyber defence framework. Changes to CSE authorities in 2001 and 2019 permitted that organization to develop a line of work that has proven critical to Canada's cyber defence. Also important were amendments made in 2004 to the *Criminal Code* and the FAA to clarify the authority of government organizations to protect their own cyber systems. This review summarizes the evolution of these authorities and instruments and the role they play in the area of cyber defence.

10. Finally, the government has provided key strategic direction, made important structural changes and invested significant resources to strengthen its cyber security and cyber defences. The government has provided strategic direction in the areas of cyber security and defence through the 2004 National Security Policy, the 2010 Cyber Security Strategy and the 2018 National Cyber Security Strategy. It made significant changes to the machinery of government, notably with the creation of SSC in 2011 and the Canadian Centre for Cyber Security in 2018. Many of these changes were accompanied by significant investments: in total, between the years 2010 and 2021, the government invested more than $6 billion in defending government networks from cyber attack.[5] This report will describe the various changes made by the government over the past two decades and recommend where efforts need to be made to complete this work, including in areas of government authorities.

[5] Canada, Budget 2021 (Chapters 9 and 10), https://www.budget.gc.ca/2021/report-rapport/toc-tdm-en.html; Budget 2019, https://www.budget.gc.ca/2019/docs/plan/chap-04-en.html#Part-4-Public-Safety-and-Justice; Budget 2018, https://www.budget.gc.ca/2018/docs/plan/chap-04-en.html#Ensuring-Security-and-Prosperity-in-the-Digital-Age; Budget 2016, https://www.budget.gc.ca/2016/docs/plan/ch5-en.html#_Toc446106818; Public Safety Canada, Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date, 2015.

Overview of the Review

11. On June 19, 2020, the Committee decided to undertake a review of the Government of Canada's framework and activities to defend its systems and networks from cyber attack. On July 6, 2020, the Chair of the Committee provided notification letters to the ministers of National Defence and Public Safety and Emergency Preparedness, and the President of the Treasury Board. The review included the following organizations:

- Communications Security Establishment;
- Shared Services Canada;
- Treasury Board of Canada Secretariat; and
- Public Safety Canada.

12. The Committee informed the ministers that the review would examine the federal framework for cyber defence, the activities that constitute cyber defence for the government, and the authorities and governance structures, including for interdepartmental governance and coordination, under which they are conducted. The objectives of the review would be to:

- examine the evolution of the legislative, regulatory, policy, operational, administrative or financial frameworks associated with the conduct of cyber defence activities;
- identify the type, nature and extent of the activities that constitute cyber defence for the government and the evolving threat they are designed to counter;
- examine the evolution of the authorities, accountability and governance structures for cyber defence activities, including interdepartmental governance and coordination;
- identify the systems and networks that constitute the government's information technology systems;
- review relevant case studies pertaining to the cyber compromise of government systems; and
- consider the risks associated with cyber defence activities (e.g., to the privacy rights of Canadians).

13. The Committee focused its inquiry on the defence of federal government systems from cyber attack, an area of examination squarely within its statutory mandate. In doing so, the Committee excluded a number of issues from the scope of its review. It did not examine cyber defence activities related to the protection of critical infrastructure outside of federal government systems (e.g., other levels of government or sectors such as energy). The protection of critical infrastructure is a large and complex topic in itself, which the Committee may examine in the future. It did not examine the government's activities in relation to the defence of the 2019 federal election from cyber threats. The government had already undertaken a report on this subject when the Committee announced its review; after receiving that report in 2020, the Committee made comments and recommendations to the Prime Minister. Finally, the Committee did not examine the government's response to cyber crime: the Royal Canadian Mounted Police, one of the core security and intelligence organizations subject to Committee

review, was in the midst of implementing significant changes in how it investigates cyber crime. Further, the majority of cyber crime does not fall within the Committee's review mandate.

14. The Committee reviewed significant amounts of historical documentation from 2001 to the present, principally to explore the evolution of the government's understanding of cyber threats and what was needed to address them. The Committee focused its analysis on key periods when major incidents forced government departments to shift operations, and when the government passed enabling legislation or made changes to the machinery of government to address cyber defence challenges. Consistent with its past reviews, the Committee placed significant emphasis on accountability, authorities, and governance and coordination of activities.

15. The Committee's review proceeded in two stages. The first was an examination of government material that described the evolution of responses to new and emerging cyber threats. The Committee supplemented this material with academic and public sources of information, but it was limited in the discussions it could hold with subject matter experts outside of government due to the pandemic. The second stage was to hold briefings and appearances with government officials. The Committee's Secretariat worked closely with relevant departments to obtain and clarify information. In total, the Committee held five meetings with various government departments and considered over 2,500 documents, representing over 37,000 pages of material.

16. This report is written in five parts. The first is a description of cyber threats facing the government and an examination of what is at stake when government networks are attacked by cyber threat actors. The second is a historical description of how the government's framework for defending its networks has evolved since 2001. That part explains the importance of statutory authorities in underpinning cyber defence activities, the role of various government policies, particularly successive cyber security strategies, and key changes in the machinery of government, notably the creation of Shared Services Canada in 2011 and the Canadian Centre for Cyber Security in 2018. The third part examines the roles, responsibilities, authorities and activities of the key players in the government's cyber defence framework: the Treasury Board of Canada Secretariat, Shared Services Canada, and the Communications Security Establishment, collectively known as the Information Technology Security Tripartite. The fourth describes the overarching governance framework for cyber defence activities in the government. Finally, the Committee provides its assessment, findings and recommendations.

17. In this latter section, the Committee notes that the government's cyber defence framework has evolved over time towards a horizontal 'enterprise' approach that treats government systems and networks as a single entity. The last ten years have shown that this evolution has improved Canada's cyber defences considerably. However, Canada cannot be complacent: the government must continue to implement the measures required to adapt to change. In particular, the horizontal approach to cyber defence is increasingly at odds with departments' vertical authorities, where individual organizations and Crown corporations retain significant discretion to opt into the government cyber defence framework or to make the

changes necessary to protect their systems from sophisticated threats. These authorities were set in a pre-digital era and should be updated for new technologies and threats.

Past Examinations of Cyber Defence Activities

External review

18. A number of reviews, audits and evaluations have been conducted on aspects of the government cyber defence framework. These were conducted by independent, external review or audit entities, parliamentary committees, the Communications Security Establishment (CSE) Commissioner (the former body dedicated to reviewing CSE activities) and bodies internal to the government. As background to the Committee's review, this section summarizes each in turn. The implementation of recommendations from these studies are not tracked as part of this review.

19. The following external reviews or audits contained specific reference to the protection of government information systems from cyber threats:

- **Office of the Auditor General of Canada – Chapter 3: Protecting Canadian Critical Infrastructure Against Cyber Threats (2012):** Part of this audit examined how the government protects its information systems and the roles and responsibilities of the departments involved. It recommended that Treasury Board of Canada Secretariat update relevant policies to reflect the new information security roles and responsibilities of Shared Services Canada (SSC).[6]
- **Office of the Auditor General of Canada – Report 4: Information Technology Shared Services (2015):** This audit examined how SSC provided information technology services to other federal departments, including information technology security. It recommended that SSC establish expectations or provide information on core elements of security to partners to allow them to comply with government information technology security policies, guidelines and standards.[7]
- **Senate of Canada Standing Committee on Banking, Trade and Commerce – Cyber Assault: It should keep you up at night (2018):** This report primarily examined how to enhance cyber security for Canadians and businesses. However, it also considered how to improve the government's cyber security framework and strengthen oversight over the many departments that have cyber security as part of their mandate. The report recommended the creation of a new federal minister of cyber security who would be responsible for Canadian cyber security policy while coordinating cyber security efforts with provincial and territorial governments and the private sector.[8]

---

[6] Office of the Auditor General of Canada (OAG), *2012 Fall Report: Chapter 3: protecting Canadian critical infrastructure against cyber threats*, 2012, https://publications.gc.ca/site/eng/9.575104/publications.html.
[7] OAG, *2015 Fall Reports: Report 4: Information Technology Shared Services, 2015, https://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html.*
[8] Senate of Canada, *Cyber Assault: It should keep you up at night*, 2018, https://sencanada.ca/en/info-page/parl-42-1/banc-cyber-security/.

The CSE Commissioner

20. Between 1996 and 2019, the CSE Commissioner was responsible for reviewing CSE activities for compliance with the law and policy direction from the Minister of National Defence. In his final report in 2019, the CSE Commissioner reported that CSE had accepted and implemented 166 of the 175 recommendations made since 1997 across all areas of CSE's mandate, a completion rate of 95 percent. Between 2001 and 2019, the CSE Commissioner conducted a number of reviews of CSE's cyber defence activities, which were variously known as active network security testing, security posture assessments, cyber defence operations and information technology security activities. In general, the CSE Commissioner examined programs or aspects of CSE's cyber defence activities to determine whether:

- ministerial authorizations for cyber defence activities met conditions specified in the *National Defence Act*;
- cyber defence activities were conducted in accordance with legislative, ministerial and policy requirements;
- CSE directed cyber defence activities at Canadians or persons in Canada; and
- if private communications intercepted by CSE were deemed essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

21. In October 2006, the CSE Commissioner noted that CSE senior management became aware that certain cyber defence activities may not have been compliant with operational policies and procedures. The Commissioner found that management paid insufficient attention to the conditions for and compliance with ministerial authorizations, and that the control framework for carrying out activities under ministerial authorization was not sufficiently clear, consistent, comprehensive or current. The cumulative impact of these issues called into question CSE's compliance with the *Privacy Act* and the *National Defence Act*. As a result, CSE suspended all cyber defence activities under ministerial authorization to conduct an internal investigation. These activities were restarted in October 2007 following a restructuring of the ministerial authorization program and policy framework.[9]

22. Since 2007, the CSE Commissioner has found that ministerial authorizations for cyber defence activities met the requirements of the *National Defence Act*, and that these activities were in accordance with the law and CSE policies.[10] The CSE Commissioner also confirmed that CSE did not direct its cyber defence activities toward Canadians or persons in Canada. Nonetheless, between 2001 and 2019 the CSE Commissioner made a number of recommendations to ensure that CSE cyber defence activities had:

---

[9] Office of the Communications Security Establishment Commissioner (OCSEC), *Review of CSEC's activities under the Protection of Computer Systems and Networks of the Government of Canada Ministerial Authorizations – CSEC's Security Posture Assessment – Active Network Security Testing (ANST) Activities in 2007–2008 and 2008–2009*, Report 58, February 14, 2011, pp. 4–5.

[10] OCSEC, *Review of CSEC's activities under the Protection of Computer Systems and Networks of the Government of Canada Ministerial Authorizations*, Report 58, February 14, 2011, p. 25.

- practical definitions, new record classifications, and clear retention and disposal schedules for personal information;[11]
- appropriate policies for filing, retaining and deleting key information found under a ministerial authorization;[12]
- improved descriptions in ministerial authorizations to clearly identify what the Minister was authorizing;[13] and
- improved clarity under the *National Defence Act* regarding authorities that risk intercepting private communications.[14]

23. In 2019, the *National Security Act* created two new organizations. The first is the National Security and Intelligence Review Agency, which took on the review activities of the CSE Commissioner. The second is the Intelligence Commissioner, who (among other things) reviews the annual cyber security authorizations granted to CSE by the Minister of National Defence.[15] These authorizations allow CSE to access the information infrastructures of federal or designated non-federal institutions where it would otherwise contravene an Act of Parliament (e.g., the *Criminal Code*) or interfere with the reasonable expectation of privacy of a Canadian or a person in Canada. Since his office was created in 2019, the Intelligence Commissioner has found all cybersecurity authorizations he has reviewed to be reasonable. However, the Intelligence Commissioner also noted that cyber security authorization applications have had several inconsistencies, including missing descriptions of outcomes, missing descriptions of the cyber security services received by clients and unexplained conditions that the Minister imposed on authorizations. These issues did not affect the Intelligence Commissioner's assessment of the reasonableness of the Minister's conclusions.

Internal review

24. The following internal reviews or audits are particularly relevant to the government's cyber defence framework:

- **Treasury Board of Canada Secretariat – Report on Cyber Security of Government Systems (2016):** This study analyzed aspects of cyber security across the government and determined there was a lack of clear decision-making at the enterprise level. It suggested nominating a senior-level executive with a mandate to resolve responsibility

---

[11] OCSEC, Report on CSE ITS Ministerial Authorizations, Report 24, May 20, 2003, pp. 31–32.
[12] OCSEC, Information Security Activities Conducted Under the Industry Canada Ministerial Authorization, Report 38, December 19, 2006, pp. 10–11.
[13] OCSEC, Privacy and Technology, Report 46, June 11, 2008, p. 24.
[14] OCSEC, Review of ITS ANST/CDO 2013, Report 89, March 31, 2015, p. 23.
[15] The Office of the Intelligence Commissioner is an independent, quasi-judicial body responsible for reviewing the conclusions of: (a) the Minister of National Defence in issuing or amending a foreign intelligence authorization or a cyber security authorization for the Communications Security Establishment; (b) the Minister of Public Safety and Emergency Preparedness in determining classes of Canadian datasets that the Canadian Security Intelligence Service (CSIS) may collect, or in determining classes of acts or omissions that CSIS may be justified in doing, which would otherwise be offenses under the CSIS Act; and (c) the Director of CSIS in authorizing CSIS to query a dataset in exigent circumstances or to retain a foreign dataset. See Office of the Intelligence Commissioner, *Annual Report 2020*, March 31, 2020, https://www.canada.ca/en/intelligence-commissioner/annualreport.html.

gaps and facilitate enterprise initiatives. It also suggested reducing redundancies among governance committees.[16]

- **Office of the Comptroller General of Canada – Horizontal Internal Audit of Information Technology Security in Large and Small Departments (2016):** Part of a multi-year, multi-phase effort, this audit reviewed governance and control frameworks over information technology security for unclassified government networks. It found that such frameworks were in place and that Treasury Board of Canada Secretariat had established policy direction for information technology security. However, the audit noted that policy instruments were out of date and that further clarification of roles and responsibilities was needed, including for SSC, to further define expectations for securing legacy systems. The audit also found that the several committees governing information technology policy instruments needed to improve coordination and reporting relationships. Additional phases were planned for the years 2019-20 to 2021-22.[17]
- **Public Safety Canada – Horizontal Evaluation of Canada's Cyber Security Strategy (2017):** This review examined the government's progress to defend against cyber attacks. It found that, despite improvements, there was still confusion between departments on their roles and responsibilities, particularly between CSE and the then-Public Safety Canadian Cyber Incident Response Centre. The private sector echoed this concern, noting that it was unclear as to where private sector organizations should report cyber incidents or seek assistance. The review also found that the government needed to continue to strengthen its ability to prevent, detect, respond to and recover from cyber attacks. It recommended that the government strengthen its horizontal governance of cyber security by re-assessing participation on existing committees and developing terms of reference to better define departmental roles and responsibilities.[18]

---

[16] References to enterprise decision-making or enterprise security initiatives refer to an Enterprise Security Architecture led by Treasury Board of Canada Secretariat that includes common, government-wide approaches to planning and delivering common security services. Essentially, it means treating the government as a single entity, rather than as a collection of individual organizations each responsible for their own cyber security and defence. In the context of cyber security, this enterprise approach enhances the government's ability to protect itself from cyber threats by standardizing security controls and improving information sharing about cyber threats, thereby supporting improved responses to cyber incidents. See Shared Services Canada (SSC), *SSC Cyber and IT Security Framework*, Version 1.0, October 8, 2014; and Public Safety Canada, Progress Report on Canada's Cyber Security Strategy – Horizontal Initiative for 2012-13 and 2013-14, undated.

[17] Office of the Comptroller General of Canada, *Horizontal Internal Audit of Information Technology Security in Large and Small Departments (Phase 1)*, 2016, https://www.canada.ca/en/treasury-board-secretariat/services/audit5-evaluation/horizontal-internal-audits/security-large-small-departments-phase-1.html.

[18] Public Safety Canada, *Horizontal Evaluation of Canada's Cyber Security Strategy*, 2017, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx.

Part I: Cyber Threats – what's at stake and who is involved?

25. As a vital part of Canada's critical infrastructure, the government collects and holds information and provides services that are of significant value to Canada's adversaries. In this digital age, nearly everything the government holds or does is potentially at risk – whether it's Canadians' tax and employment information, companies' proprietary and research data, and government policies, investigations and operations, or the electronic processes that underpin the many services and benefits on which Canadians depend. Government networks are therefore integral to Canada's national security. This chapter describes what is at stake for cyber threats to government systems, the evolution of cyber threats over time, and the most significant threat actors facing Canada today. It is a primer for the rest of this review.

What's at stake?

26. Cyber attacks against government systems threaten the information held by the government and the various electronic systems and processes it needs to function. This broad vulnerability can be broken into five areas, each of which will be described in the following paragraphs:

- personal information of Canadians;
- proprietary information, intellectual property and research of Canadian businesses and researchers;
- government policies and policy-making;
- security and intelligence information and operations; and
- integrity of government systems.

Threats to the personal information of Canadians

27. The government collects and manages significant amounts of personal information. This includes names, dates of birth, addresses, social insurance information, passport information, health records, voting information and many other personal details. For example:

- the Canada Revenue Agency holds information related to Canadians' identity, income, employment, benefits and taxes;
- Immigration, Refugees and Citizenship Canada holds information related to individuals' identity and status in Canada; and
- the Canada Border Services Agency holds sensitive Advance Passenger Information/Passenger Name Record Data, entry-exit information and biometric information (fingerprints and digital photographs) for certain categories of travellers.

Criminals could use such data to impersonate Canadians, open bank accounts, apply for loans or credit cards, or obtain government benefits or refunds.[19] Hostile foreign states could use this data to track Canadians or persons living in Canada.[20]

Threats to business information, intellectual property, research networks and academia

28. The government holds information related to Canadian businesses, intellectual property, research networks and academia. For example:

- the National Research Council possesses information related to Canadian advancements in technology and intellectual property that can be vital to the technical success of Canadian and international companies;
- Defence Research and Development Canada holds information on defence science and technology – including that developed or shared with partner departments, industry, academia and international allies – that is used to support defence and security operations at home and abroad; and
- Innovation, Science and Economic Development Canada possesses information related to Canada's conditions for investment, innovation and international trade.

The theft of this data by malicious actors could undermine Canada's international competitiveness and economic interests, sap innovation and harm national security.

Threats to government policies and policy-making

29. The government holds information related to its policies and policy-making. Through various policy- and decision-making processes, the government generates and obtains significant and often very sensitive information on topics spanning its domestic and international work, such as foreign policy and trade, defence and security, natural resources, energy, and finance. The same is true for processes and decisions that may affect, for example, financial markets or foreign investments, including budgetary planning and regulations, or involve Canada's judicial system. For example:

- Global Affairs Canada holds information related to Canada's bilateral and multilateral relations, international trade, consular cases, and peace and security assistance efforts;
- Treasury Board of Canada Secretariat possesses information related to government spending, regulation and management in the areas of people, money and technology;

---

[19] Canada Revenue Agency, *Protect Yourself Against Identity Theft*, 2010, www.canada.ca/en/revenue-agency/services/forms-publications/publications/rc284/protect-yourself-against-identity-theft.html.
[20] For additional information, see National Security and Intelligence Committee of Parliamentarians (NSICOP), *Annual Report 2020*, 2021, https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html.

- the Department of Finance holds information related to economic and fiscal matters, including the annual budget, tax and tariff policy, social measures, and security-related investments; and
- the Federal Court holds information on deliberations regarding administrative law; citizenship, immigration and refugee law; intellectual property; maritime law; and national security (e.g., warrants authorizing certain activities of the Canadian Security Intelligence Service).

This information is of interest to foreign states or criminals. If stolen, it could jeopardize Canada's national interests, international competitiveness and negotiating positions, reputation on the world stage, and international relations. The theft of decision-making and finance documents could reveal information related to the government's spending and programming plans, undermine its international negotiation strategies, and jeopardize trust in Canadian markets. Cyber attacks targeting court processes could divulge sensitive records and deliberations, threatening the integrity of the legal system.

Threats to security and intelligence information and operations

30. Government networks hold information related to Canada's national security, intelligence and defence activities, including operations and investigations. For example:

- the Canadian Security Intelligence Service holds highly classified information, including national security investigations on specific states and individual Canadians, and as part of the government's security clearance process, it collects sensitive information on government employees who require access to classified information or sensitive sites; and
- the Department of National Defence and the Canadian Armed Forces hold information on Canada's military operations, technology and equipment, strategies, intelligence, and procurement plans.

The theft of information related to military operations could reveal military strategies, targets, operations and plans, potentially jeopardizing the safety of Canada's troops abroad and the success of military operations. The theft of information related to security and intelligence operations and investigations could reveal the identities of security and intelligence officials, jeopardizing their safety and making them targets for extortion or espionage. The loss of such information could also risk divulging intelligence-gathering sources and methods, inhibiting Canada's ability to gather intelligence on threats to national security.

Threats to the integrity of government systems

31. Finally, a successful cyber attack could compromise the integrity of government systems. As a key part of Canada's critical infrastructure, the government must provide services without disruption. Ensuring the continuity of government is essential across numerous areas. For example:

- the Prime Minister, Cabinet, individual ministers and parliamentarians rely on information technology and electronic communications to conduct sensitive state business;
- Employment and Social Development Canada, Service Canada and their partner departments rely on information technologies to provide numerous benefits to Canadians, including pensions, passports, Employment Insurance, and disability benefits for veterans; and
- Shared Services Canada provides backbone and digital services to government organizations in order to deliver digital programs and services across a range of mandates.

A cyber attack against government systems could jeopardize the continuity of government, the delivery of services and the integrity of information holdings. The economic and social well-being of Canadians would suffer as a result.

What's happening? The cyber threat environment

32. The Communications Security Establishment (CSE) defines a **cyber threat** as "an activity intended to compromise the security of an information system by altering the availability, integrity or confidentiality of a system or the information it contains." **Cyber threat actors** conduct cyber threat activities. These actors are composed of "states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information and systems in order to access or otherwise affect victims' data, devices, systems, and networks."[21] CSE identifies six types of cyber threat actors, based on their primary motivation:

- **Nation-states:** motivated by a range of strategic, political, security or economic objectives, states try to obtain advantages in the economic, political or military spheres;
- **Cybercriminals:** motivated by a real or perceived monetary reward, criminals seek to make money from targeting vulnerabilities;
- **Hacktivists:** driven by a sense of activism, hacktivists try to draw attention to their political or social cause;[22]
- **Terrorist groups:** motivated by violent extremism grounded in religious or political sentiment, terrorists seek to fundraise, proselytize and plan attacks;
- **Thrill-seekers:** motivated by a sense of personal satisfaction, thrill seekers try to 'beat' the cyber defences of an organization or government; and

[21] Communications Security Establishment (CSE), An Introduction to the Cyber Threat Environment, 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf.
[22] Translation Bureau, Public Services and Procurement Canada, "Hacktivist," Termium Plus data bank, 2021. www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=hacktivist&index=ent&codom2nd_wet=1#resultrecs

- **Insider threats:** driven by discontent and dissatisfaction, insider threats seek revenge for past slights or profit from selling secrets.[23]

33. Cyber threat actors are not equal in their capability or sophistication. Key differentiators are access to technical and financial resources and training. Threat actors in the top tier of sophistication and skill are called **advanced persistent threats**. They use advanced techniques to conduct complex and protracted campaigns in the pursuit of their strategic goals. Nation-states are typically the most sophisticated threat actors, with their expansive state resources, advanced (and often highly classified) technologies, extensive planning and coordination, and the ability to operate with near legal impunity. With few exceptions, cybercriminals are generally understood as moderately sophisticated threat actors, although they may still use dedicated planning, support and technical capabilities to conduct activities against a large number of victims. Hacktivists, terrorist groups and thrill-seekers are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Insider threats are individuals who work as trusted employees within organizations, but could cause significant loss of data or system disruption owing to their access to internal (and otherwise protected) networks.[24] While the Committee recognizes that the government must defend its systems against any threat, regardless of sophistication or motivation, in this review the Committee focuses primarily on state-sponsored actors due to their high-level of sophistication and therefore greatest possibility of causing significant harm.

34. The **cyber threat environment** is the online space where cyber threat actors conduct malicious cyber threat activity.[25] This environment is made up of technological components, including Internet connectivity and connected devices, computing power and data storage, and the people and organizations that use them, including governments, citizens, businesses, universities and industries. This threat environment has evolved over time, the most notable changes being the exponential growth in users, bandwidth, computers and other devices, and a corresponding increase in the creation of personal and proprietary data.[26]

35. Government departments and agencies have increased interconnectivity among themselves and with external Internet environments, such as private sector organizations and citizens. This interface between government networks and external cyber environments is essential for the government to provide services to clients. In fact, it is at the very core of the government's vision for digitally based operations, one where programs and services are available digitally to all Canadians, anytime, anywhere and from any device.[27] This also exposes

---

[23] CSE, An Introduction to the Cyber Threat Environment, 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf; and CSE, Government of Canada Enterprise Security Architecture Enterprise Threat Assessment, January 2017.
[24] CSE, An Introduction to the Cyber Threat Environment, 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf.
[25] CSE, An Introduction to the Cyber Threat Environment, 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_e.pdf.
[26] Canadian Centre for Cyber Security (CCCS), Modern Ransomware and Its Evolution, 2020
[27] For additional information on the government's vision for digital operations, see the Digital Operations Strategic Plan: 2018-2022 at https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/digital-operations-strategic-plan-2018-2022.html#ToC3.

government systems and networks to deliberate threat actors that may target the government with malicious cyber activity; it also means that a cyber compromise of one department may threaten others.

36. Cyber threat actors attack information systems using a number of methods. As CSE notes, "the structure of the Internet makes it possible for a threat actor to connect directly to an information system from across the globe or to monitor communications associated with a target information system."[28] For example, cyber threat actors could:

- monitor an interaction between two devices or software components in the information system, resulting in a compromise of data;
- deny communication between two components, halting the provision of critical services;
- insert themselves between two devices or modules that are communicating and intercept their communications; or
- gain access to government systems by impersonating a legitimate user or by stealing login credentials.[29]

37. The balance between cyber defence and offence varies. Government departments use a variety of Internet browsers, software, applications and hardware, all of which vary in age and sophistication and require constant updating and maintenance to limit vulnerabilities, and have implemented sophisticated measures to strengthen defences. At the same time, threat actors have become more capable of launching cyber attacks. For relatively unsophisticated cyber threat actors, hacking tools have become cheaper and more readily available through criminal service providers, making it easier to conduct sophisticated, hard-to-detect attacks.[30] As described later, the most sophisticated threat actors, notably China and Russia, continue to adapt their capabilities to subvert defensive measures, and other states, such as ***, are investing heavily in their capacity to do the same. In short, cyber threats to government networks and the measures necessary to block them rapidly evolve.

Cyber threats to government networks, 2015 to 2020

38. In its *Annual Report 2020*, the Committee described the contemporary landscape of malicious cyber activities threatening government systems, critical infrastructure providers, the private sector and Canadians.[31] In this review, the Committee's analysis will more narrowly describe malicious cyber activities that targeted government systems and networks from 2015 to 2020.

---

[28] CSE, Government of Canada Enterprise Security Architecture Enterprise Threat Assessment, 2017.
[29] CSE, Government of Canada Enterprise Security Architecture Enterprise Threat Assessment, 2017.
[30] CSE, *Operational Threat Report: 2019 Annual Threat Landscape – 1 January to 31 December 2019*, 2020. CSE notes that cyber crime is one of the fastest-growing forms of transnational crime and suggests that it will continue to expand as the increasing availability of malware lowers the technical expertise needed to cause harm.
[31] NSICOP, *Annual Report 2020*, 2021, https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html.

39. CSE identifies threats to government systems in two ways. CSE's foreign intelligence program monitors foreign cyber actors to identify their techniques and interests (among other things). That information is shared with the Canadian Centre for Cyber Security (CCCS), which is housed within CSE. For its part, CCCS manages three types of cyber defence sensors, which scan for known threats and anomalies across certain government departments, networks and cloud environments. CCCS combines information from these sources with information shared by partners to create indicators of compromise that allow it to identify potential malicious cyber threats in the future.[32] As the deployment of cyber defence sensors has increased over time, CCCS's ability to detect malicious cyber activity on government systems has also grown.

40. The same is true for CCCS's ability to block that activity. Beginning in 2013 (before CCCS was created), CSE started to deploy network-based dynamic defences, a ground-breaking shift in defensive capability. Dynamic defences allowed CSE to move beyond only identifying threats to proactively blocking them. To create these defences, newly identified threats are *** updated into CSE's dynamic defence system. The sensors can then detect those threats and launch mitigation actions automatically to block them. Although malicious threat actors continue to target the government, the deployment of these dynamic defences has significantly reduced their success in compromising government systems.[33] In appearances before the Committee, CCCS officials stated that the volume of cyber incidents has gone down since 2015 and that the impact of such incidents has become less significant, owing to CCCS's ability to respond quickly to new attacks and prevent the type of damage that in the past would have required targeted departments to completely rebuild their networks.[34] Officials also stated that in the early 2010s, CSE observed thousands of incidents per year, which included a number of cases of data exfiltration from Government of Canada networks. They added, "Now, if we see *** a year, it's a bad year, because we are able to intervene very quickly."[35] The evolution and deployment of sensors is described later in this review.

Evidence of compromise

41. There are a number of malicious activities that indicate that a network has been compromised. *** These include beaconing, remote exploitation, malware artifacts, malware download, phishing, browser-based exploitation, data exfiltration, remote access, and denial of service. Each is described below.[36]

Beaconing

42. Beaconing is a method of communication between a compromised target network and the attacker's computer. A threat actor deploys a beacon through numerous means, including

---

[32] CCCS, Review of the Government of Canada's Cyber Defence Activities, NSICOP appearance, February 19, 2021.
[33] CSE, *Year Review Cyber Defence Report 2017*, 2018.
[34] CCCS, Remarks of the CCCS Head, NSICOP appearance, February 19, 2021.
[35] CCCS, Remarks of the CCCS Head, NSICOP appearance, February 19, 2021.
[36] Of note, CSE's methodology for tracking malicious cyber activity has evolved over the years as its knowledge of cyber threat actors has grown and as it has expanded its deployment of cyber defence sensors to additional government departments. Where CSE has been able to identify and describe malicious cyber threat activity, it refers only to those portions of government networks on which it has visibility: departmental traffic traversing the Shared Services Canada (SSC) Enterprise Internet Service or data derived from its host-based cyber defence sensors.

remote exploitation, phishing or browser-based exploitation. The purpose of the beacon is to alert the threat actor that the attack was successful and that the tool the actor implanted was able to circumvent network defences (e.g., a firewall). In turn, that allows the threat actor to create other communication channels (usually hidden and encrypted) to introduce additional, more advanced tools (for example, to further exploit the network or to steal information).[37] [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment. ***].[38]

Remote exploitation

43. Remote exploitation is the process where a threat actor sends a set of commands from a remote network to a target device to gain access to that device or to the information it holds.[39] In general, remote exploitations take advantage of vulnerabilities or weaknesses in software, hardware or the configuration of a computer or network device. Essentially, a remote exploit is the way the criminal picks the lock.[40] [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment. ***].[41]

Remote access

44. Remote access refers to unauthorized remote connections to a victim host by a threat actor without the use of an exploit (e.g., by using a valid username and password pair, often illegitimately obtained through data theft or the successful delivery of a phishing email).[42] Legitimate users interact with files, information and system resources when working remotely (e.g., telework).[43] By leveraging remote access to a target network, malicious cyber threat actors can mimic all of the interactions and activities of a legitimate user. [*** Two sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment. ***].[44]

Malware artifacts and downloads

45. Malware refers to a wide range of malicious software designed to infiltrate or damage a computer system, without the owner's consent.[45] A malware tool can be deployed via multiple means (e.g., remote exploitation, phishing or browser-based exploitation). Malicious software (code) is "written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system."[46] Malware artifacts are detectable traces of

---

[37] CCCS, "Glossary," www.cyber.gc.ca/en/glossary. See also the "beaconing" definition at, International Association of Chiefs of Police, Law Enforcement Cyber Centre, https://www.iacpcybercenter.org/resources-2/glossary/#B.
[38] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape – 1 January to 31 December 2019*, 2020.
[39] CCCS, "Glossary," www.cyber.gc.ca/en/glossary.
[40] Vice, https://www.vice.com/en/article/mg79v4/hacking-glossary.
[41] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; CSE, "NSICOP Cyber Report – Typos and Small Changes," pp.1, July 9, 2021.
[42] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[43] Techtarget, "Remote Access," Search Security, https://searchsecurity.techtarget.com/definition/remote-access#:~:text=Remote%20access%20is%20the%20ability,distance%20through%20a%20network%20connection.&textA%20VPN%20creates%20a%20safe,network%2C%20such%20as%20the%20internet.
[44] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[45] CCCS, "Glossary," www.cyber.gc.ca/en/glossary.
[46] Global Knowledge, "Cyber Security Glossary of Terms," https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/#top.

malware on a victim's device.[47] Malware downloads refers to instances in which malware was downloaded onto a *** device.[48] [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment. ***] (see Figure 1).[49]

Source: CSE, *Year Review Cyber Defence Report*, 2016; CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

Figure 1: [*** This figure was deleted to remove injurious or privileged information. The figure depicted data collected by CSE. ***]

Phishing

46. Phishing involves state-sponsored threat actors and cybercriminals soliciting confidential information from specific targets to trick them into disclosing personal data or credentials.[50] Phishing activity can be conducted with official-looking emails (known as spear-phishing) that can vary in sophistication and often contain malicious links or files that, when opened, infect the recipient's computer with malware. A threat actor may use this malware to access a target's computer to steal information, or use the target's personal information (e.g., account credentials, credit card information) to access banking information or perform identity theft.[51]

47. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSE's assessment. ***].[52]

Browser-based exploitation

48. Web browsers and associated applications contain flaws and vulnerabilities that malicious cyber actors use to gain control of a target computer when it connects to an infected website. These actors then proceed to steal user credentials, deliver ransomware, execute malware, steal information or obtain permissions on a network to access other devices.[53] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described a CSE capability and assessment. ***].[54] [55] [56]

---

[47] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[48] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[49] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019. [*** One sentence was deleted to remove injurious or privileged information. The sentence described a CSE capability. ***] See CSE, Year Review Cyber Defence Report 2017, 2018
[50] CCCS, "Glossary," www.cyber.gc.ca/en/glossary.
[51] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; CCCS, "Glossary," https://www.cyber.gc.ca/en/glossary.
[52] CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[53] Cynet, "Browser Exploits – Legitimate Web Surfing Turned Death Trap," https://www.cynet.com/blog/browser-exploits-legitimate-web-surfing-turned-death-trap/.
[54] Of note, CSE is able to [*** The rest of this sentence was deleted to remove injurious or privileged information. It described a CSE capability. ***]
[55] CSE observed an increase in browser-based exploitation in 2019, attributed to a specific ransomware distribution campaign. CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[56] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.

Data exfiltration

49. Data exfiltration is the unauthorized removal (theft) of information from a target network once a threat actor has gained access through means such as remote exploitation.[57] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment. ***].[58] [59]

Denial of service

50. Denial of service is a technique used to prevent legitimate users from accessing a network-connected service by sending illegitimate requests to overload a network's resources.[60] [*** Two sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment. ***].[61]

Nation-state advanced persistent threats

51. CSE tracks the cyber activities of a number of state actors. China and Russia represent the most sophisticated cyber threat actors targeting the government.[62] Iran, North Korea and *** have moderately sophisticated capabilities and *** pose less-sophisticated threats. Advanced persistent threat actors can be part of the formal apparatus of a state (e.g., a military unit, intelligence or security agency), or a non-state entity directed and supported (e.g., financially) by a state. The former are known as state actors and the latter are known as state-sponsored actors.[63] For simplicity, the Committee uses the name of the involved state when discussing both state actors and state-sponsored actors (e.g., "China"). The evolution of these advanced persistent threats from 2015 to 2020 is discussed below. (Note: CSE classifies a threat as 'high, moderate or low' based on its knowledge of the technological sophistication of the threat actor and its assessment of the probability that specific threat actors will target Canada.)

China

52. China is a highly sophisticated cyber threat actor. Its primary strategic objectives are maintaining internal stability and developing as a global power. It has three priorities:

- collection of intelligence to inform the government's foreign, trade and security policies;

---

[57] International Association of Chiefs of Police, Law Enforcement Cyber Centre, "Glossary," https://www.iacpcyberCentre.org/resources-2/glossary/#E; and CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[58] CSE, *Year Review Cyber Defence Report 2017*, 2018.
[59] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[60] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[61] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019.
[62] When assessing the level of threat state-sponsored actors pose to the government, CSE bases its assessment on a combination of three factors: technical sophistication of cyber capabilities, organizational capacity and degree of interest.
[63] Threat Post, "Defending Against State and State-Sponsored Threat Actors," https://threatpost.com/defending-against-state-threat-actors/162518/; and CSE, An Introduction to the Cyber Threat Environment, https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

- collection of research and academic information for strategic technologies that could benefit China's economy or military; and
- collection of ***.[64]

CSE assessed that "the scope and tenacity of [Chinese] activity in pursuit of Canadian intellectual property, proprietary information, and government positions and policies cannot be overstated." It noted that China's cyber activity was "aggressive and vast" and "more audacious" than previously witnessed. [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment of China's capabilities. ***].[65]

53. *** China continued to be *** a prolific threat actor targeting the government. Consistent with its intelligence priorities, China targeted multiple government sectors, including security, intelligence and defence (***); international affairs, trade and development (***); industry and business development (***); government administration (***); transportation (***); and natural resources, energy and environment (***).[66] Since the start of the COVID-19 pandemic, China has targeted research networks in the United States, United Kingdom and Canada. ***.[67]

54. China uses a range of techniques to target government systems and networks. [*** Four sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment of China's capabilities. ***].[68] [69] [70] In short, it has adapted its techniques to respond to the particular defensive posture of its targets.

55. *** CSE observed a wide range of Chinese malicious cyber activity and the layering of techniques. [*** Three sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment of China's capabilities. ***].[71] In sum, China continues to be a highly sophisticated and active cyber threat.[72]

---

[64] CCCS, Cyber Threat Brief: State Activity Against Canada, January to June 2020, 2020.
[65] CSE, Cyber Threat Update: People's Republic of China and Russia, 2015; and CSE, *Annual Cyber Report 2015*, 2016.
[66] CSE, Year Review Cyber Defence Report, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020; and CCCS, Cyber Threat Brief: State Activity Against Canada, June to December 2020, 2021.
[67] CCCS, Cyber Threat Brief: State Activity Against Canada January to June 2020, 2020.
[68] *** CSE, *Quarterly Cyber Defence Report Q1 2015*, 2015.
[69] CSE, Cyber Threat Update: People's Republic of China and Russia, 2015; and CSE, *Annual Cyber Report 2015*, 2016.
[70] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[71] ***
[72] CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; CCCS, *Cyber Threat Report: State-Sponsored Targeting Trends Report 2018 Annual*, 2019; CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020; and CCCS, Cyber Threat Brief: State Activity Against Canada, June to December 2020, February 11 2021

Russia

56. Russia is a highly sophisticated cyber threat actor. Russia engages in malicious cyber threat activity, including *** cyber espionage and foreign interference, to support a wide range of strategic intelligence priorities. These include:

- foreign and military intelligence collection against diplomatic, economic and military targets, including private sector entities and academic institutions;
- reconnaissance of critical infrastructure industrial control systems and telecommunications providers; and
- identification of divisive events and trends in rival states to conduct influence campaigns and undermine liberal democratic norms and values.[73]

Russia also employs a number of non-state actors, including cybercriminals, private companies and so-called troll farms to conduct cyber threat activities on its behalf. [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment of Russian priorities. ***].[74]

57. *** Russia was among the most prolific state-sponsored threat actors targeting the government. Consistent with Russia's strategic intelligence priorities, its cyber threat activity has been directed at a number of sectors, including consistent targeting of: international affairs, trade and development (***); security, intelligence and defence (***); and natural resources, energy and environment (***).[75] In 2020, Russia targeted the Canadian health sector to steal intellectual property related to COVID-19 vaccine development and pharmaceutical research. [*** One sentence was deleted to remove injurious or privileged information. The sentence described CSE's assessment. ***].[76]

58. [*** This paragraph was revised to remove injurious or privileged information. The paragraph described CSE's assessment of Russia's capabilities, and noted that Russia employs a wide range of tactics in its targeting of government systems and networks and that Russia remains a highly sophisticated and active cyber threat to government networks. ***].[77] [78] [79] [80] [81] [82]

---

[73] CCCS. Cyber Threat Brief: State Activity Against Canada, January to June 2020, 2020.
[74] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[75] CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[76] CCCS, Cyber Threat Brief: State Activity Against Canada – January to June 2020, 2020.
[77] CSE, *Annual Cyber Report 2015*, 2016.
[78] CSE, *Year Review Cyber Defence Report 2016*, 2017.
[79] CSE, *Year Review Cyber Defence Report 2017*, 2018; and CSE, CCCS, *Cyber Threat Report: State-Sponsored Targeting Trends: Report, 2018 Annual*, 2019.
[80] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[81] CSE, *Annual Cyber Report*, 2015; CSE, *Year Review Cyber Defence Report*, 2016; CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020. ***
[82] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

Iran

59. Iran poses a moderate cyber threat. [*** This paragraph was revised to remove injurious or privileged information. The paragraph described CSE's assessment of Iran's capabilities, and noted four sectors where Iran focused its cyber activities. ***].[83] [84] [85] [86]

North Korea

60. North Korea poses a moderate cyber threat. North Korea acts similarly to cybercriminals, stealing cryptocurrencies and fiat currencies to fund the government and its officials. [*** Two sentences were deleted to remove injurious or privileged information. The sentences described CSE's assessment. ***].[87] [88]

***

61. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSE's assessment of a state that poses a moderate cyber threat. ***].[89] [90] [91]

***

62. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSE's assessment of a state that poses a low cyber threat. ***].[92] [93]

---

[83] CSE, *Year Review Cyber Defence Report, 2017*, 2018.
[84] CCCS, *Cyber Threat Report: State-Sponsored Targeting Trends Report, 2018 Annual*, 2019. *** CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; CCCS, *Cyber Threat Report: State-Sponsored Targeting Trends Report, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[85] CCCS, Cyber Threat Brief: State Activity Against Canada January to June 2020, 2020.
[86] CCCS, Cyber Threat Brief: State Activity Against Canada January to June 2020, 2020
[87] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[88] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020; CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020; CCCS, Cyber Threat Brief: State Activity Against Canada January to June 2020, 2020.
[89] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[90] CCCS, ***, 2019.
[91] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020; and CSE, NSICOP Cyber Defence Review, Request for Information-4, Item #3 – Question Related to State-Sponsored Threat Actor, June 2, 2021.
[92] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[93] CSE, *Annual Cyber Report*, 2015; CSE, *Year Review Cyber Defence Report*, 2016; CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

***

63. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSE's assessment of a state that poses a low cyber threat. ***].[94] [95]

***

64. [*** This paragraph was deleted to remove injurious or privileged information. The paragraph described CSE's assessment of a state that poses a low cyber threat. ***].[96] [97]

Government networks and cyber crime

65. The government is increasingly aware of the threat posed to its systems by cyber crime. Cyber crime is one of the most prevalent cyber activities affecting government networks, systems and users, as it is a low-risk, high-reward activity. Availability and access to new technologies have significantly lowered the cyber crime entry barrier, making it easier for amateur cybercriminals to launch sophisticated and hard-to-detect attacks.

66. CSE examined cyber crime activity targeting the government for the first time in a classified format in its *2019 Annual Threat Report.* It assessed that the government is an attractive target for cybercriminals for a number of reasons. First, government networks are home to numerous databases containing valuable information on a wide range of subjects, such as financial information, intellectual property and personal information. Second, the sheer size of government systems and networks means that opportunistic cyber actors that cast a wide net across the Internet are bound to target the government. Third, governments at all levels may be an attractive target for extortion, particularly via ransomware, owing to large departmental budgets and obligations to citizens that may force a government to pay a ransom in some cases.[98] [*** The rest of this paragraph was revised to remove injurious or privileged information. The paragraph described CSE's assessment of the extent of ransomware attacks as a proportion of all cyber crime targeting government networks. While relatively low, CSE noted that even a single successful ransomware compromise could be devastating for an individual department. It identified one recent attack against a government department, which was contained, and another against a Canadian Crown corporation, which caused considerable

---

[94] CCCS, Canada's Cyber Threat Landscape: Overview and Outlook for 2019, 2019.
[95] CSE, *Year Review Cyber Defence Report 2017*, 2018; and CCCS, *Cyber Threat Report: State-Sponsored Targeting Trends Report, 2018 Annual*, 2019.
[96] CCCS, Canada's Cyber Threat Landscape: Review of 2019 and Outlook for 2020, 2020.
[97] CSE, *Annual Cyber Report*, 2015; CSE, *Year Review Cyber Defence Report*, 2016; CSE, *Year Review Cyber Defence Report*, 2017; CCCS, *Cyber Defence Report: Government of Canada IT Compromises and Vulnerabilities, 2018 Annual*, 2019; and CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[98] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020. In its explanation of this point, CSE stated that ***

harm. The paragraph notes that the government is currently considering a policy on ransomware payments. ***].[99] [100] [101]

Summary

67. Government of Canada networks are a vital part of Canada's critical infrastructure. The government uses them to collect and hold information and to provide services that are of fundamental importance to Canadians and Canadian businesses. The information they hold is also of significant value to Canada's adversaries, including state-sponsored cyber threat actors and cybercriminals. In this digital age, nearly everything the government holds or does is potentially a target for malicious cyber activity, from a wide range of data on Canadians and businesses to the electronic processes that underpin the many services and benefits on which Canadians depend. The following sections describe government efforts to strengthen its cyber defences and reduce Canada's vulnerabilities.

[99] CCCS, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[100] CSE, NSICOP Cyber Defence Review, RFI-3, Ransomware and GC Depts, 2021.
[101] Treasury Board of Canada Secretariat (TBS), Remarks of a senior official, NSICOP Secretariat meeting, March 23, 2021; and TBS, "NSICOP Review - TBS Comments on Draft Final Report (9-July-2021)," pp. 1, July 9, 2021.

Part II: Evolution of the Government's Framework for Cyber Defence

68. The evolution of the government's framework for cyber defence has been a mix of unanticipated and reactionary, and deliberate and planned. Changes in legislation provided new authorities that drove the development of activities to strengthen the security of government systems and eventually better defend them. At the same time, major cyber threat actors forced the government to adapt its defences, particularly following critical cyber incidents that caused significant loss of data and underlined the vulnerability of individual departments and the government more generally. The government responded by promulgating key strategies and policies, investing in the modernization of information technology and cyber defences, and creating organizations specifically tasked with addressing weaknesses in the system. In the process, the government progressively moved away from its siloed approach where individual departments, no matter how big or small, were responsible for their own cyber defence, to treating the government as an "enterprise," where specific organizations are responsible for driving the implementation of government-wide policies and for providing "defence in depth" services to protect the government as an organization.

Early days (2001 to 2010)

69. The genesis of cyber defence in Canada was legislative. On December 18, 2001, Parliament passed the *Anti-Terrorism Act*. As its name suggests, the Act was a response to the terrorist attacks of September 2001. For the Communications Security Establishment (CSE), it meant that its mandate and authorities were enshrined in statute (the *National Defence Act)*,[102] permitting a significant expansion of its foreign intelligence activities to support, among other things, the fight against al-Qaida. At the same time, the Act provided CSE with broad authority to provide advice, guidance and services to protect electronic information and information infrastructures of importance to the government, including ministerial authorizations for activities that would risk intercepting private communications. Over time, this authority allowed CSE to develop and conduct novel cyber defence activities on government computer systems or networks, notably active network security testing to *measure* the security of specific government systems and networks and computer network defence activities to *protect* specific government systems and networks.[103]

---

[102] *National Defence Act*, R.S.C., 1985, c. 95, s.s. 273.64(1) and 273.64(2) (prior to passage of Bill C-59 and the *Communications Security Establishment Act*), http://laws-lois.justice.gc.ca/eng/acts/n-5/20181218/P1TT3xt3.html.
[103] *National Defence Act*, R.S.C., 1985, c. 95, s.s. 273.65(9) (prior to passage of Bill C-59 and the *Communications Security Establishment Act*), http://laws-lois.justice.gc.ca/eng/acts/n-5/20181218/P1TT3xt3.html. The Act explicitly limited the application of the ministerial authorization regime to "federal institutions" as defined in the *Official Languages Act*.

Active network security testing and security posture assessments

70. From 2002 to 2012, CSE offered active network security testing activities to government departments. These activities involved CSE using various *unclassified* technical methods to penetrate the computer systems of a government institution to identify vulnerabilities and weaknesses in a network and to test the reaction of the department to an active cyber threat. These "penetration" tests were designed to determine if a cyber threat actor (played by CSE) could access a network and obtain sensitive or classified documents that should not have been publicly available. The results were used to make recommendations to remedy deficiencies.[104]

71. CSE conducted its first activities under ministerial authorizations in 2002. It tested for vulnerabilities in *** CSE's own networks and for weaknesses in *** networks at CSE and the Privy Council Office.[105] In November 2002 and April 2003, CSE obtained ministerial authorizations to conduct similar tests against networks at the Canadian Security Intelligence Service (CSIS) and the Department of Foreign Affairs and International Trade, respectively. Based on this experience, CSE began using its authorities in earnest. Between 2002 and 2006, CSE obtained 11 ministerial authorizations to conduct testing and assessment activities of the systems for the following organizations:

- Department of National Defence, including *** (October 2002);
- Royal Canadian Mounted Police (June 2003);
- Privy Council Office (November 2003);
- Canada Customs and Revenue Agency (December 2003);
- Department of Human Resources Development (January 2004)
- Department of National Defence (January 2004);
- Industry Canada (May 2004);
- *** (October 2004)
- CSE, including the networks of the Office of the CSE Commissioner (April 2005);
- Privy Council Office (February 2006); and
- Department of National Defence (February 2006).[106]

These activities were halted in October 2006. When they were restarted in December 2007, CSE used a different approach (paragraphs 74–76).

---

[104] CSE Commissioner, Combined Review of CSE activities under the 2009-2010, 2010-2011, and 2011-2012 Active Network Security Testing and Cyber Defence Operations Ministerial Authorizations, March 31, 2015. The methods used to conduct active network security testing relied on cyber tools that were known to hackers at the time, ***

[105] CSE, "Security Posture Assessment," Ministerial authorization, April 23, 2002; CSE, "Security Posture Assessment: CSE and PCO," Ministerial authorization, April 23, 2002; and CSE, "Request for Ministerial Authorization. Protection of CSIS Information Systems and Networks," Memorandum for the Minister of National Defence, October 25, 2002.

[106] CSE, "Security Posture Assessment: CSIS," Ministerial authorization, November 2, 2002; and CSE, "Protection of the Computer Systems or Networks of the Government of Canada (DFAIT)" Ministerial authorization, March 26, 2013.

The origin of computer network defence activities

72. [*** This paragraph was revised to remove injurious or privileged information. ***] Between 2004 and 2006, CSE began conducting activities that would form the basis of its cyber defence program. In late 2003, the Department of National Defence (DND) identified intrusions (later identified as Russia) against its systems and requested CSE assistance. In January 2004, CSE sought the Minister's authorization to conduct normal active network security testing activities on the DND network and to deploy cyber defences to identify attempted exploitations and monitor the activities of the advanced cyber threat actor.[107] In the same year, CSE and Foreign Affairs Canada (FAC) had been tracking attempts by China to compromise the FAC network. In June 2005, CSE sought the Minister's authorization to deploy cyber tools on FAC systems.[108]

73. In 2006, CSE received ministerial authorizations to conduct computer network defence activities on the DND networks (February), FAC networks (June) and its own networks (June). CSE attributed the increasingly sophisticated attacks against DND networks to China, and the attacks against FAC networks to both China and Russia. As it had done *** in 2004, CSE *** deployed tools to enhance its capacity to detect sophisticated cyber attacks against government networks, to respond to such attacks, and to pursue the (foreign) origins of detected attacks through CSE's foreign intelligence activities.[109] This was the birth of advanced, computer network defence activities in the Government of Canada, what today is called "cyber defence activities."

Hard lessons learned along the way

74. In October 2006, CSE suspended all of its active network security testing and computer network defence activities. As the CSE Commissioner later explained,

> CSE did not fully comply with the requirements and conditions of [its ministerial authorizations (MAs)] during the period June 2005 to October 2006. Insufficient management attention was paid to the conditions of the MAs, to their communication, and to compliance with them. The control framework for those carrying out these activities was not sufficiently clear, consistent, comprehensive, or current. The

---

[107] CSE, "Protection of Computer Systems and Networks of the Department of National Defence," Ministerial authorization, January 19, 2004; CSE, "Request for Ministerial Authorization. Protection of DND Computer Systems and Networks," Memorandum for the Minister of National Defence, January 19, 2004; and CSE Commissioner, Combined Review of CSE activities under the 2009-2010, 2010-2011, and 2011-2012 Active Network Security Testing and Cyber Defence Operations Ministerial Authorizations, March 31, 2015.

[108] CSE, "Request for Ministerial Authorization. Protection of Government of Canada Computer Systems and Networks: Foreign Affairs Canada," Memorandum for the Minister of National Defence, June 16, 2005; and CSE, "Protection of Government of Canada Computer Systems and Networks: Foreign Affairs Canada," Ministerial authorization, June 22, 2005.

[109] CSE, "Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks. Communications Security Establishment," Memorandum for the Minister of National Defence, June 2006; and CSE, "Protection of Government of Canada Computer Systems and Networks," Ministerial authorization, June 13, 2006.

cumulative impact of these issues called into question CSE compliance with the *Privacy Act* and the *National Defence Act*.[110]

CSE reviewed its programs and implemented several changes over the course of a year to restructure its activities and policy framework, and improve program monitoring and accountability.

75. In December 2007, CSE requested ministerial authorization to resume active network security testing activities. CSE moved from a department-by-department request for authorities to an umbrella approach of a single ministerial authorization that permitted CSE to provide network security assessments at the request of any government department, consistent with the Treasury Board Government Security Policy.[111] CSE continued to offer these services to government departments until 2012, when it was clear that the relative value of network penetration tests had declined (CSE was *always* able to penetrate its test subject networks). CSE shifted its focus exclusively to cyber defence, where its defences were making considerable progress on identifying and blocking sophisticated cyber attacks.

76. In March 2008, the Minister of National Defence approved a similar umbrella request for ministerial authorization to resume computer network defence activities on government networks to protect against the theft of sensitive information by advanced cyber actors. CSE noted that an expanding number of government departments were being victimized by highly sophisticated adversaries, particularly China and Russia. CSE was authorized to conduct five types of computer network defence activities under the authorization:

- **incident analysis:** the investigation of alerts when CSE's classified intrusion detection system flagged possible threats;
- **anomaly analysis:** the creation of standardized profiles for government departments and their network traffic to identify abnormal behaviour that may indicate malicious activity;
- **forensic intrusion analysis:** the detailed examination of malicious network intrusions to identify potential harm to a government network;
- **incident reporting:** the provision of mitigation advice stemming from identified intrusions; and
- **advanced tool development:** the enhancement of CSE's classified intrusion detection tools based on the analysis of malicious cyber activity to improve detection of cyber threats.[112]

---

[110] CSE Commissioner, Combined Review of CSE activities under the 2009-2010, 2010-2011 and 2011-2012 Active Network Security Testing and Cyber Defence Operations Ministerial Authorizations, March 31, 2015.
[111] CSE, "Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks," Memorandum for the Minister of National Defence, December 21, 2007; CSE. *Ministerial Authorization. Protection of Government of Canada Computer Systems and Networks*. December 21, 2007; TBS, Government Security Policy, February 2002, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322.
[112] CSE, "Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks," Memorandum for the Minister of National Defence, February 29, 2008; and CSE, "Defence of Government of Canada Computer Systems and Networks," Ministerial authorization, March 11, 2008.

As is detailed later, this shift enabled CSE to deploy its sensors to the government's Secure Channel Network, which consolidated Internet access for over 70 departments. As a result, CSE discovered that China had compromised a number of departments and stolen significant amounts of data. This discovery was the catalyst for a number of changes in the following years (described below), including to push more departments under CSE's defences.[113] For its part, CSE continues to offer its computer network defence activities to government departments and has done so under successive ministerial authorizations since 2008. Today, these are known as cyber defence activities, described in more detail in the CSE section (paragraphs 154–213).

Government policies for cyber defence

77. Between 2001 and 2010, the government released two policies of significant relevance to cyber defence: the Government Security Policy in 2002 and the National Security Policy in 2004. The Government Security Policy was intended to support the national interest and the government's business objectives by safeguarding employees and assets and assuring continued service delivery. This policy stated that deputy heads are accountable for safeguarding employees and assets under their responsibility and established a number of baseline security requirements that deputy heads must follow. Among these requirements, departments must appoint a departmental security officer to establish a security program that ensures coordination of all policy functions including information technology security, security screening and access limitations. The Government Security Policy obligated departments to implement baseline information technology security controls to prevent, detect, react to and recover from the compromise of information technology systems. Importantly, departments had to conduct periodic security evaluations of their information technology systems, continuously monitor the operations of these systems to detect anomalies in service delivery levels, and establish mechanisms to respond effectively to information technology incidents, should they arise, and exchange incident-related information with lead departments in a timely manner.[114] Treasury Board updated the Government Security Policy in 2009 and again in 2019, when it was renamed the Policy on Government Security. Its contemporary relevance and application is described in paragraphs 103–106.

78. The government's *National Security Policy* provided a strategic framework and action plan to ensure that the government was prepared to respond to a range of national security threats. The Policy described cyber attacks as "a growing concern that have the potential to impact on a wide range of critical infrastructure that is connected through computer networks." To address this threat, the document introduced two initiatives: first, to substantially improve threat and vulnerability analyses for government systems and to strengthen its ability to defend government systems from attacks; second, to develop a National Cyber-Security Strategy.[115] These initiatives were funded in later Budgets.

---

[113] SSC, "SCNet Enterprise Internet – 2010 and 2011," TBS CIOB communique, February 24, 2021.
[114] TBS, Government Security Policy, February 2002, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12322. The policy applied to all departments listed in schedules I, I.1, and II of the *Financial Administration Act*.
[115] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, April 2004, www.publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

Establishing the government enterprise (2010 to 2018)

79. The period between 2010 and 2018 was critical to the establishment of the government's cyber defence framework. During this time, the government introduced two national cyber security strategies and allotted significant funding toward cyber defence and cyber security. The government also made significant changes to its organizational structure with the creation of Shared Services Canada and the Canadian Centre for Cyber Security. At the same time, major cyber attacks were important catalysts for change, including the growing deployment of CSE's defensive sensors on government networks and the consolidation of government data centres and Internet access points. The government also established mechanisms to govern cyber defence and clarified the roles and responsibilities of respective players in the cyber defence framework. These changes are described below.

Canada's Cyber Security Strategy, 2010

80. In October 2010, the government released Canada's Cyber Security Strategy to defend Canadians, Canadian businesses and the economy from cyber threats. The strategy had three pillars:

- **Securing government systems:** intended to strengthen the government's ability to prevent, detect, respond to and recover from cyber threats.
- **Partnering to secure vital cyber systems outside government:** intended to strengthen cyber resiliency in Canada, including for critical infrastructure sectors.
- **Helping Canadians to be secure online:** intended to promote public awareness, educate Canadians on how to protect themselves online and strengthen the ability of law enforcement agencies to combat cyber crime.[116]

The strategy received over $244 million in funding over five years, and $60 million annually thereafter.[117] The most relevant pillar to cyber defence was the first: securing government systems. Under it, there were three notable outcomes: strengthening CSE's cyber defence program, the creation of Shared Services Canada, and implementing better governance and policies. Each are addressed in turn below.

Strengthening CSE's cyber defence program

81. The primary goal of the first pillar of the strategy was to increase the government's cyber technology, intelligence analysis and investigative capacity. The majority of funding, $205 million over five years (84 percent of total funding for the strategy), was provided to CSE to enhance its ability to defend government systems and networks. This included installing new network-based sensors to monitor departments' networks for cyber threats and automatically

---

[116] Canada, Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada, 2015.
[117] Public Safety Canada, Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date, 2015.

mitigate cyber attacks, and developing host-based sensors, software designed to defend individual government devices.[118]

82. These investments significantly improved CSE's cyber defence capabilities. Prior to the strategy, CSE's cyber defence program focused on incident response and mitigation, which involved labour-intensive manual processing and ad hoc reporting to individual clients. With the deployment of network-based dynamic defence in 2013, CSE was better able to monitor and analyze threat information that it could then use proactively to prevent cyber attacks from reaching government users and systems by blocking attacks at the government perimeter. The merit of this tool was underlined in 2014, when CSE deployed its dynamic defence network-based sensors on the Shared Services Canada Secure Channel Network to support the government's efforts to mitigate a major cyber vulnerability (see case study 3 on HEARTBLEED). Under the strategy, CSE had established the Cyber Threat Evaluation Centre to improve its awareness and understanding of sophisticated cyber threats targeting government systems.[119] This allowed CSE to better track and report on known cyber threats and trends and to automate the discovery of cyber threats and the deployment of defences.[120] The development of CSE's cyber defence program has contributed to a steady expansion of the visibility of government networks to CSE and a simultaneous decrease in the number of successful data exfiltrations.[121]

Creating Shared Services Canada

83. The creation of Shared Services Canada (SSC) facilitated the implementation of the objectives outlined in Canada's Cyber Security Strategy.[122] This change contributed significantly to the evolution of the government's cyber defence architecture, as it consolidated information technology resources from 42 departments (approximately 95 percent of all federal resources) and accelerated the shift toward an enterprise approach to cyber security. In general, SSC is responsible for designing and operating secure information technology infrastructure that protects government data and technology assets; developing security policies, standards, plans and designs; and providing security-related services for the delivery of government services.[123] As part of the strategy, SSC increased its capacity to provide threat monitoring, vulnerability assessment and computer forensic services for its 43 core partners and deployed new tools to assist in handling the increasing volume of cyber threats (see section on SSC, paragraphs 126-153).[124] Notably, SSC also consolidated more than 720 government data centres to 381, with a

---

[118] Public Safety Canada, Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date, 2015.
[119] Public Safety Canada, Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date, 2015
[120] CSE, Cyber Threat Evaluation Centre Overview, March 2015.
[121] CSE, *Year Review Cyber Defence Report 2017*, 2018.
[122] Canada, Action Plan 2010-2015 for Canada's Cyber Security Strategy, 2013. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx.
[123] SSC, Cyber and Information Technology Security, 2015. www.canada.ca/en/shared-services/corporate/cyber-information-technology-security.html.
[124] Public Safety Canada, Update on the Implementation of the 2010 Cyber Security Strategy, 2011.

goal to ultimately transition to 4 regional hubs, and reduced the number of Internet access points from approximately 100 to 2, with plans to add 3 regional hubs (for a total of 5 secure connections) and potentially 3 international hubs. Reducing these points of vulnerability made the protection of the entire government cyber enterprise easier. Through its Federal Information Protection Centre, SSC provided threat monitoring, coordinated all security incidents affecting SSC's supported infrastructure, and consolidated incident reporting from its core partners. The creation of SSC and the consolidation of departments into a government enterprise model has increased the government's awareness of cyber threats and vulnerabilities and established conditions for more uniform deployment of CSE's sophisticated cyber defence sensors.[125]

Implementing better governance and policy

84. Governance was another key feature of the 2010 cyber strategy. Prior to the strategy, governance of cyber defence was marked by a lack of clarity concerning roles and responsibilities and a largely ad hoc and decentralized model, with deputy ministers individually responsible for the cyber security and cyber defence of their respective organizations.[126] One of the objectives of the 2010 strategy was to establish clear roles and responsibilities for the management of cyber events. To this end, Public Safety Canada and CSE re-aligned their responsibilities related to incident coordination and management, making Public Safety Canada responsible for performing cyber security management for non-federal entities, including the provision of mitigation advice to other levels of government (at the time, the Strategy focused on engagements with provincial and territorial governments) and the private sector, and CSE responsible for performing cyber security operations and cyber incident management for government systems.[127]

85. For its part, the Treasury Board of Canada Secretariat (TBS) established three governance committees to provide information technology security governance for horizontal initiatives under the first pillar of the 2010 strategy. Known as the Information Technology Security Tripartite, these committees were created at the Director General, Assistant Deputy Minister and Deputy Minister levels and are further described in paragraphs 221-223. TBS also led the development of an improved Information Technology Incident Management Plan to enable more rapid and integrated government-wide response to cyber security incidents. This plan identified departmental roles and responsibilities for reporting and responding to information technology incidents; formalized horizontal reporting, warning and response protocols; and identified senior committees and officials to be engaged when threats escalated

---

[125] Public Safety Canada, *Progress Report on Canada's Cyber Security Strategy: Horizontal Initiative for 2012-13 and 2013-14*, undated; and Public Safety Canada, *Horizontal Evaluation of Canada's Cyber Security Strategy. Final Report*, September 29, 2017.

[126] Public Safety Canada, Cyber Operations Working Group Terms of Reference. 2010; and Public Safety Canada, Options for Government of Canada: Centralized Cyber Security Functions, 2010.

[127] CSE and Public Safety Canada, "Memorandum of Understanding Between The Communications Security Establishment Canada and Public Safety Canada Concerning Cyber Security Roles and Responsibilities," 2011.

in severity.[128] Governance of incident management further evolved in 2015 as the government replaced this plan with the new Cyber Security Event Management Plan (paragraphs 224–236).

86. As roles and responsibilities were better understood and departmental coordination increased, the government created a number of interdepartmental governance mechanisms. The primary governance mechanism for policy matters was the Deputy Ministers' Committee on Cyber Security (DM Cyber Security), which was supported by committees at the assistant deputy minister and director general levels. These three committees were chaired by senior Public Safety Canada officials; their membership consisted of senior officials from CSE, TBS, SSC, CSIS, the Royal Canadian Mounted Police, DND / Canadian Armed Forces, and the Privy Council Office. The purpose of DM Cyber Security was to establish policy direction for issues related to cyber security, set cyber security-related priorities for member departments and agencies, and consider emerging cyber security issues.[129] In terms of outcomes, a 2016 evaluation found that this governance structure facilitated collaboration, coordination and information-sharing among participating organizations, and helped to clarify departments' roles and responsibilities. However, the evaluation could not determine the extent to which governance bodies fulfilled their stated purposes, including holding regular meetings, due to an absence of proper documentation. It also found that uncertainty regarding roles and responsibilities persisted, causing confusion for departments, agencies and private sector stakeholders, and that information-sharing was selective or ad hoc due to the absence of specific policies.[130]

87. TBS supported effective governance and the response to cyber incidents by establishing operational standards, guidelines and policies. In 2016, TBS released the Information Technology Strategic Plan. This plan guides federal organizations on information technology priority-setting and decision-making, including in the area of information technology security. Relevant priority initiatives in this area included securing the government's network perimeter, implementing endpoint security profiles, and implementing a systematic approach to vulnerability and patch management.[131] TBS also released the first iteration of its Digital Operations Strategic Plan in 2018. This plan sets the direction for departments on the priorities for the integrated management of services, information, data, information technology and cyber security. From a cyber security and cyber defence perspective, the plan mandates the development of a layered approach that uses trusted interconnection points to provide a gateway to cloud services.[132]

---

[128] Treasury Board of Canada Secretariat, Government of Canada Information Technology Incident Management Plan, 2009.
[129] Public Safety Canada, Deputy Ministers' Committee on Cyber Security Terms of Reference, March 2015.
[130] Public Safety Canada, Horizontal Evaluation of Canada's Cyber Security Strategy Final Report, 2017, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx.
[131] TBS, Government of Canada Information Technology Strategic Plan 2016-2020, 2016, www.canada.ca/en/treasury-board-secretariat/services/information-technology/information-technology-strategy/strategic-plan-2016-2020.html#toc8.
[132] For more detailed information, see TBS, Digital Operations Strategic Plan 2018-2022, March 29, 2019, www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html.

The evolution of Canada's Cyber Security Strategy

88. In 2015, the government renewed its 2010 cyber security strategy. This renewal marked the second phase of the strategy and was meant to address three challenges. First, the strategic cyber threat environment had evolved considerably, with the emergence of more capable cyber threat actors and an increase in the proliferation of cyber tools. Second, cyber security had become a major economic issue as cyber threat actors had increasingly targeted Canadian businesses. Third, there was an increasing need to keep Canadians safe online through better digital literacy and new approaches to cyber crime. To address these challenges, the government provided funds for three initiatives:

- increasing cyber threat intelligence collection and analysis in order to share threat information with critical infrastructure and private sector systems;
- increasing partnership with telecommunications service providers for conducting assessments of cyber vulnerabilities and dependencies in critical infrastructure; and
- dedicating law enforcement capacity to more effectively investigate and disrupt cyber crime.[133]

These initiatives fell within pillars two and three of the 2010 cyber security strategy – partnering to secure vital cyber systems outside of the government, and helping Canadians to be secure online – areas that had received less funding. Specific funding was also devoted to address security gaps highlighted by China's cyber attack against the National Research Council in 2014 (see case study 4).[134]

89. In June 2018, the government announced its new National Cyber Security Strategy. The 2018 strategy was based on a government-wide evaluation of the 2010 strategy and included input from private sector experts, law enforcement and academics. The 2018 strategy defined three goals to achieve security and prosperity in the digital age:

- **Secure and resilient Canadian systems:** intended to improve the government's ability to protect Canadians from cyber crime, respond to evolving cyber threats, and help defend critical government and private sector systems;
- **An innovative and adaptive cyber ecosystem:** intended to support research, foster innovation and develop cyber skills to position Canada as a global leader in cyber security; and
- **Effective leadership, governance and collaboration:** intended to advance cyber security and work with allies to shape the international cyber security environment in Canada's favour.[135]

---

[133] Public Safety Canada, Renewal of Canada's Cyber Security Strategy, August 20, 2015.
[134] Public Safety Canada, Renewal of Canada's Cyber Security Strategy, August 20, 2015.
[135] Public Safety Canada, Introducing the 2018 National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age, undated.

The 2018 strategy's core goals and initiatives were reflected in Budget 2018's investments in cyber security, which totalled $508 million over five years and $109 million annually thereafter. Most notably, CSE received $155 million over five years and $45 million annually thereafter to create a new centre for cyber security.

90. In response, the government created the Canadian Centre for Cyber Security (CCCS) in October 2018. This change consolidated the roles and responsibilities of a number of federal cyber organizations, notably CSE's Information Technology Security program, Public Safety Canada's Canadian Cyber Incident Response Centre and its public awareness campaign, and some functions of SSC's Security Operations Centre. CCCS has four primary responsibilities:

- **inform** Canadians about cyber security matters, including cyber security threats;
- **protect** Canadian interests through advice, assistance and collaboration with partners across the country and abroad;
- **defend** networks and systems that are within its visibility; and
- **develop** and enrich the knowledge, personnel and skills needed to continually improve cyber security for Canadians.[136]

CCCS is meant to serve as a single source of government advice, guidance, services and support on cyber security operational matters. It is the government's operational lead during cyber security events and is intended to provide more coordinated and focused government responses to cyber threats and incidents; improve coordination of government cyber security activities; and provide more effective information exchanges between the government and private sector partners.

91. The 2018 strategy included a number of initiatives related to protecting Canada's critical infrastructure. The strategy's five-year action plan directs CCCS to improve its partnerships with owners and operators of critical infrastructure in the finance and energy sectors to enable the exchange of cyber security knowledge and capabilities to better defend against advanced cyber threats.[137] It also directs Public Safety Canada to deliver a comprehensive risk management approach to enable critical infrastructure owners and operators to better secure their systems and information. Finally, the strategy included funding for CSIS to increase its work in cyber intelligence collection and cyber threat assessments to improve its cyber situational awareness and ability to provide advice to the government on issues of cyber relevance.[138]

92. The government's framework for cyber defence continues to evolve. In June 2019, the *Communications Security Establishment Act* received Royal Assent, significantly changing CSE's mandate, authorities, immunities and oversight, including in areas of immediate relevance to cyber defence. In April 2020, Treasury Board released its Policy on Service and

---

[136] CSE, Presentation to Col. Peyton, April 10, 2018.
[137] Public Safety Canada, National Cyber Security Action Plan, *2019-2024*, 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntl-cbr-scrt-strtg-2019/ntl-cbr-scrt-strtg-2019-en.pdf.
[138] Public Safety Canada, National Cyber Security Action Plan, *2019-2024*, 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntl-cbr-scrt-strtg-2019/ntl-cbr-scrt-strtg-2019-en.pdf.

Digital, which establishes the rules by which the government will manage service delivery, information and data, information technology, and cyber security in the digital era. These changes will be addressed in the following sections on TBS and CSE, respectively.

Part III: Key Cyber Defence Players, Authorities and Activities

93. Cyber security is a shared responsibility across government. While individual departments are responsible and accountable for the security of their information technology assets, three key organizations carry out specific government-wide responsibilities and services, including for the narrower mandate of cyber defence. Known as the Government of Canada Information Technology Security Tripartite, these organizations are the Treasury Board of Canada Secretariat (operating at the direction of the Treasury Board), Shared Services Canada and the Communications Security Establishment.

94. This section examines the roles, responsibilities, functions and cyber defence activities of the Information Technology Security Tripartite in detail. It delineates the responsibilities of individual departments for cyber security, based on an expansive view of the scope of entities that make up the Government of Canada. An analysis of the legislative regimes, administrative policies and other authorities of the Tripartite organizations related to providing cyber defence services to government entities identifies which entities can receive cyber security and cyber defence services, and to what degree. This approach facilitated a broad understanding of the responsibilities, activities and range of protection of the government's cyber defence framework.

Treasury Board of Canada and the Treasury Board of Canada Secretariat

95. Established as a Cabinet committee in 1869, the Treasury Board of Canada plays a foundational role in Canada's cyber defence framework. The Treasury Board prescribes the policies, standards and directives for cyber defence and determines to which organizations these requirements apply. Treasury Board's enabling legislation, the *Financial Administration Act* (FAA), provides roles and responsibilities for key officials across government and broadly sets a number of the policy, administrative and accountability pillars of the government's cyber defence framework.

96. Treasury Board exercises a broad mandate across government. Under the FAA, it is responsible for departmental accountability and financial management in the administration of government and for regulatory oversight of government programs and services; it is also the primary employer for the Government of Canada. The FAA sets out the requirements for a number of key officials and enables the Treasury Board, through the Treasury Board of Canada Secretariat (TBS), to issue policies, directives, standards and guidelines for the management and administration of the majority of federal organizations. The Treasury Board is also responsible for monitoring departmental management practices and program results, including in areas of security policy. Though historically Treasury Board has played a nominal role in matters of national security, its functions regarding the management and administration of government make it a central player in the cyber defence framework.

97. The FAA defines broad roles and responsibilities. These include the President of the Treasury Board, the Secretary of the Treasury Board of Canada Secretariat (the department's deputy head), and the Chief Information Officer of Canada (the CIO of Canada). Their key roles and responsibilities include the following:

- **President of the Treasury Board**: serves as the Chair of the Treasury Board and sets the agenda for the government in the areas of people, money and technology. The President is also responsible for TBS as a department and sets the strategic direction of the organization.
- **Secretary of the Treasury Board of Canada Secretariat**: serves as the Secretariat's deputy head and is appointed by the Governor in Council. The Treasury Board may delegate any powers or functions to the Secretary that it is authorized to exercise under any Act of Parliament or order made by the Governor in Council. The Secretary provides guidance on the interpretation of policies, directives or standards prescribed by the Treasury Board.
- **CIO of Canada**: exercises specific government-wide leadership responsibilities for the direction, oversight and capacity building for information management, information technology, government security and government service delivery, including monitoring departmental management practices, and reporting on the implementation of enterprise-wide objectives and strategic direction, including in areas of cyber security. The Treasury Board may also delegate to the CIO any powers or functions that it is authorized to exercise under any Act of Parliament or order made by the Governor in Council in relation to information technology.[139] In fulfilling this mandate, the Office of the CIO of Canada has a staff of approximately 195 people and a budget of approximately $31 million, with 21 percent ($6.4 million) allocated specifically to cyber and security policy needs.[140]

98. For their part, deputy heads of federal institutions must ensure that their departments deliver on the government's priorities and agenda, while maintaining program and service integrity. For cyber defence, this includes the responsibility of ensuring that departmental systems and networks are secure.

Defining government organizations

99. Treasury Board identifies 169 federal organizations and an additional 100 federal "interest" organizations.[141] Understanding how the government defines its own size and scope is critical to determining and assessing which organizations are subject to Treasury Board policies

---

[139] *Financial Administration Act*, R.S.C., 1985, c. F-11, https://laws-lois.justice.gc.ca/eng/acts/f-11/index.html; and TBS, Cyber Defence Review: Briefing for NSICOP, NSICOP appearance, November 27, 2020.
[140] TBS, Chief Information Officer (CIO) of Canada remarks, NSICOP appearance, November 27, 2020; TBS, "NSICOP Review – TBS Comments on Draft Final Report (9-July-2021)," pp.2, July 9, 2021; TBS, Policy on Service and Digital, April 1, 2020, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603.
[141] TBS, GC Info Base, Inventory of Federal Organizations and Interests. June 16, 2021. Https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-eng.html#igoc/inst_form, Version: ca58508.

and their obligations to secure systems and networks, and ultimately the degree to which they are protected within the cyber defence framework.

100. The FAA groups most federal organizations into specific categories, or "schedules," based on their mandate, responsibilities and relationship to government. The following six FAA schedules are of direct relevance as Treasury Board uses them to determine the applicability of policies, standards and guidelines for cyber security and cyber defence:

- **Schedule I** consists of "Ministerial Departments." Legislation establishes these organizations with mandates that cover large areas of public policy. They are assigned one or more Cabinet ministers, and are financed through parliamentary appropriations. Notable examples include the Department of Public Safety and Emergency Preparedness, the Department of Foreign Affairs, Trade and Development, and the Department of National Defence.
- **Schedule I.1** consists of "Departmental Agencies" and "Agents of Parliament." These entities typically have more narrowly defined mandates and generally operate with varying degrees of independence. Notable examples include the Communications Security Establishment, the Canadian Security Intelligence Service and Shared Services Canada.
- **Schedule II** consists of "Departmental Corporations" and "Service Agencies." Departmental corporations include organizations that perform highly operational services for which there is usually no private sector competition. They have varying levels of autonomy and management structures. Notable examples include the Canada Border Services Agency, the Canadian Nuclear Safety Commission and the Transportation Safety Board of Canada. Service agencies consist of three specialized entities established through legislation and financed through parliamentary appropriations and some user fees: the Canada Revenue Agency, the Canadian Food Inspection Agency and Parks Canada.
- **Schedule III** consists of "Parent Crown Corporations." These organizations operate on a private sector model, but have a mix of commercial and public policy objectives. Crown corporations are directly owned by the Government of Canada. Notable examples include the Canada Mortgage and Housing Corporation, Export Development Canada and VIA Rail Canada. There are nine additional parent Crown corporations not listed in this schedule of the FAA that have separate governance models established by legislation.[142]
- **Schedules IV and V** consist of additional "Portions of the Core Public Administration" and "Separate Agencies." These include organizations to which Part I of the *Canada Labour Code* does not apply or those where a minister, Treasury Board or the Governor in Council is authorized to establish the terms and conditions of employment. Notable

[142] These nine organizations are the Bank of Canada, the Canada Council for the Arts, the Canada Pension Plan Investment Board, the Canadian Broadcasting Corporation, the Canadian Race Relations Foundation, the International Development Research Centre, the National Arts Centre Corporation, the Public Sector Pension Investment Board and Telefilm Canada.

examples include the offices of the Information Commissioner and Privacy Commissioner (Schedule IV) and the Canada Revenue Agency (Schedule V, but also under Schedule II). While portions of these entities may be captured in the preceding schedules, schedules IV and V include other separate or stand-alone federal entities not listed previously.[143]

The FAA defines a department as an organization listed in schedules I and I.1 (above), any departmental corporation, and a variety of other organizations and staffs.[144] Treasury Board also uses this definition to determine the applicability of certain policy instruments for cyber defence. As discussed later, entities falling under Schedule III are not subject to those instruments.

101. The government holds an interest in a number of other organizations in addition to those listed in the FAA. These "interests" generally include organizations where the government may share ownership or participate in their management and oversight but where they are not considered formally part of the government.[145] Examples of federal interests include the Canadian Institute for Health Information, the Halifax Port Authority and the Greater Toronto Airports Authority. Notably, the House of Commons and Senate are not considered government entities and are therefore not subject to the FAA or Treasury Board policies: ***.

Foundational policies for cyber defence

102. Under the FAA, Treasury Board issued two primary policy instruments and a strategic plan that together set the administrative foundations of the government's cyber security and cyber defence posture. These are the Policy on Government Security, the Policy on Service and Digital, and the Digital Operations Strategic Plan.[146] These policy instruments and their subsidiary components are applicable to a variety of federal organizations. As part of this administrative structure, deputy heads and departments are responsible for securing their systems and networks in accordance with these policies. In instances where departments do not comply with these policies, deputy heads may apply administrative measures, ranging from persuasion (e.g., maintaining a dialogue with the non-compliant department) to restraint (e.g., reorganization of an institution or termination of employment).[147] Although the Committee observed instances of non-compliance with TBS direction, TBS did not provide examples of

---

[143] The information used to describe these six schedules is from TBS, Overview of federal organizations and interests, https://www.canada.ca/en/treasury-board-secretariat/services/reporting-government-spending/inventory-government-organizations/overview-institutional-forms-definitions.html, August 16, 2016, and the *Financial Administration Act*, R.S.C., 1985, c.F-11, https://laws-lois.justice.gc.ca/eng/acts/f-11/index.html.

[144] In the latter category, these include commissions of inquiry established under the *Inquiries Act*; staffs of the House of Commons, Senate and Library of Parliament; offices of the Senate Ethics Officer, the Conflict of Interest and Ethics Commissioner, and the Parliamentary Budget Officer; and the Parliamentary Protective Service. *Financial Administration Act*, R.S.C., 1985, c. F-11, https://laws-lois.justice.gc.ca/eng/acts/f-11/index.html

[145] TBS, Overview of federal organizations and interests, August 16, 2016, https://www.canada.ca/en/treasury-board-secretariat/services/reporting-government-spending/inventory-government-organizations/overview-institutional-forms-definitions.html.

[146] TBS, "Cyber Defence Review: Briefing for National Security and Intelligence Committee of Parliamentarians," Deck, NSICOP appearance, November 27, 2020.

[147] Treasury Board, Framework for the Management of Compliance, 2009. www.tbs-sct.gc.ca/pol/doc-eng.aspx?id+17151.

administrative consequences imposed in the context of non-compliance with the above-noted policy instruments. As the CIO of Canada emphasized during a hearing with the Committee, "Deputy heads are the ones who are ultimately responsible for meeting the requirements outlined in our [Treasury Board] policies. In particular, they have responsibility to ensure the protection and confidentiality of the information and assets within departments."[148]

Policy on Government Security

103. The Policy on Government Security has two primary objectives. The first is "to effectively manage government security controls in support of the trusted delivery of Government of Canada programs and services and in support of the protection of information, individuals and assets." The second is "to provide assurance to Canadians, partners, oversight bodies and other stakeholders regarding security management in the Government of Canada."[149] The current version of the policy was issued July 1, 2019, and is applicable to 110 federal organizations.[150]

104. The policy prescribes a series of requirements for departments and officials. It makes the Treasury Board responsible for establishing and overseeing a whole-of-government approach to security management; providing policy leadership, advice and guidance for government security; and providing strategic policy oversight and coordination of security events that may affect the government as a whole.[151] For federal organizations, it requires deputy heads to appoint a chief security officer who is responsible for providing leadership, coordination and oversight of departmental security activities.

105. Under the policy, deputy heads must approve a three-year security plan that sets out a strategy for meeting departmental security requirements. This plan must address eight security controls, which are administrative, operational, technical, physical or legal measures for managing security risks. Of the eight security controls, four relate specifically to cyber security and cyber defence:

- **Information technology security** requirements, practices and controls must be defined, documented, implemented, assessed, monitored and maintained throughout all stages of an information system's life cycle to provide reasonable assurance that information systems can be trusted to adequately protect information, are used in an acceptable manner, and support government programs, services and activities.
- **Business continuity management** is conducted systematically and comprehensively to provide reasonable assurance that in the event of a disruption, the department can

---

[148] TBS, CIO of Canada, NSICOP appearance, November 27, 2020.
[149] TBS, Policy on Government Security, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578.
[150] The Policy on Government Security is applicable to those organizations listed in schedules I, I.1 (Column I), II, IV and V of the FAA.
[151] TBS, Policy on Government Security, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578; and TBS, Terms of Reference: Implications for TBS and Collection Methodology, August 31, 2020.

maintain an acceptable level of delivery of critical services and activities, and can achieve the timely recovery of other services and activities.

- **Information management security** requirements, practices and controls are defined, documented, implemented, assessed, monitored and maintained throughout all stages of the information life cycle to provide reasonable assurance that information is adequately protected in a manner that respects legal and other obligations, and balances the risk of injury and threats with the cost of applying safeguards.
- **Security event management** practices are defined, documented, implemented and maintained to monitor, respond to and report on threats, vulnerabilities, security incidents and other security events, and ensure that such activities are effectively coordinated within the department, with partners and government-wide, to manage potential impacts, support decision-making and enable the application of corrective actions.[152]

106. In addition to these broad requirements, the Policy on Government Security shapes the government's administrative framework for cyber defence through the creation of detailed, subsidiary directives, standards and guidance. For example, the Directive on Security Management flows from the Policy on Government Security. Among a range of requirements, the directive defines the security roles and responsibilities of the chief security officer, senior officials, security practitioners and employees across the government and includes a number of detailed appendices that further refine cyber security controls.[153] One of these appendices is Mandatory Procedures for Information Technology Security Control, which sets out information technology requirements and practices, project management practices, life cycle and supply chain integrity, security assessments and authorizations, and monitoring and corrective actions.[154] In short, the Policy on Government Security and its subsidiary instruments help set the foundation for government cyber security and cyber defence.

Policy on Service and Digital

107. The Policy on Service and Digital is the second primary policy instrument in the government's cyber security and cyber defence framework.[155] Issued on April 1, 2020, it "serve[s] as an integrated set of rules that articulate how Government of Canada organizations manage service delivery, information and data, information technology, and cyber security in the digital era."[156] Together with its subsidiary Directive on Service and Digital, it consolidates and replaces a number of previous policies and directives.[157] Of note, the policy is applicable to 87

---

[152] The content of these four bullets is from TBS, Policy on Government Security, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578.
[153] TBS, Directive on Security Management, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611.
[154] For more information, see the Directive on Security Management and its supporting tools at: www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611.
[155] The Policy on Service and Digital is issued pursuant to section 7 of the FAA, as previously noted, and section 31 the *Public Service Employment Act* (PSEA). The authority to issue the policy pursuant to the PSEA relates to Treasury Board's authority as the government's employer to establish qualification standards that it deems necessary for the work to be performed in relation to this Policy.
[156] TBS, Policy on Service and Digital, August 2, 2020, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603.
[157] The policies and directives that were replaced are the Policy Framework on Information and Technology; Policy on Management of Information Technology; Policy on Information Management; Policy on Service; Policy on Acceptable

federal organizations, a narrower area of applicability than the Policy on Government Security.[158] Given the recent issuance of the policy, these organizations have an implementation period of two years to ensure compliance.

108. The Policy on Service and Digital includes a number of delegated authorities from the Treasury Board to specific officials:

- The President of the Treasury Board has the authority to issue, amend and rescind directives related to the policy.
- The CIO of Canada has the authority to issue, amend and rescind standards, mandatory procedures and other appendices related to the policy, and to enhance the government's framework to defend its networks from cyber attack.

109. The Policy on Service and Digital further defines the roles and responsibilities of key senior officials for the governance and administration of cyber security and cyber defence. The Secretary of the Treasury Board is responsible for establishing and chairing the Deputy Minister Committee on Enterprise Priority and Planning, a senior-level body that provides advice and recommendations on a number of information technology issues, including cyber security.[159] The CIO of Canada must:

- define cyber security requirements to ensure that government and departmental information and data, applications, systems, and networks are secure, reliable and trusted;
- manage cyber security risks for the government and direct "a deputy head to implement a specific response to cyber security events, including assessing whether there has been a privacy breach, implementing security controls, and ensuring that systems that put the Government of Canada at risk are disconnected or removed, when warranted;" and
- approve an annual enterprise strategic plan for the integrated management of data, information technology, information and cyber security. The latest such plan, known as the Digital Operations Strategic Plan 2018–2022, is examined further below.[160]

110. The Policy on Service and Digital gives deputy heads and departments numerous responsibilities for information technology. They must prepare an annual information technology strategic plan that is aligned with the CIO of Canada's Digital Operations Strategic Plan (see paragraphs 119–124) and monitor their organization's compliance with the Policy on Service and Digital and its supporting instruments. Deputy heads also have clearly defined responsibilities for cyber security. They must establish clear governance and reporting

---

Network and Device Use; Directive on Management of Information Technology; Directive on Information Management Roles and Responsibilities; and Directive on Recordkeeping.

[158] The Policy on Service and Digital is applicable to those organizations listed in schedules I, I.1 (Column I) and II of the FAA.

[159] TBS, Deputy Minister Committee on Enterprise Priorities and Planning Terms of Reference. Undated.

[160] TBS, Policy on Service and Digital, August 2, 2020, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603.

requirements, including the designation of an official responsible for leading the departmental cyber security management function: the Designated Official for Cyber Security. The subsidiary Directive on Service and Digital and the Guideline for Service and Digital define the roles and responsibilities of this designated official. For example, the designated official, in collaboration with the departmental chief information officer and the departmental chief security officer, provides department-wide leadership, coordination and oversight for integrating cyber security requirements to protect information technology services.[161] The designated official must also establish roles and responsibilities for reporting cyber security events (defined as an event that may be detrimental to government security, including threats, vulnerabilities and security incidents).[162]

111. Taken collectively, the Policy on Service and Digital and its subsidiary instruments require officials to enhance program delivery by leveraging new services and technologies while prescribing key cyber security and cyber defence functions and responsibilities. An important example is the government's recent Cloud Adoption Strategy and corresponding cyber security and cyber defence direction included in the Direction on the Secure Use of Commercial Cloud Services.

Using and securing cloud services: Direction from the CIO of Canada

112. Cloud-based services enable individuals and organizations to use software, hardware and services that can be hosted separately from an entity's facilities, and managed by private sector organizations.[163] As TBS describes:

> Cloud computing can be compared to public utilities that deliver commodities such as electricity. Instead of buying and running infrastructure itself, an organization buys computing power from a provider. Much like electricity in a home, cloud computing is on-demand and the consumer pays for what they use. The cost of the infrastructure used for delivery (storage and services in the case of cloud computing, hydro poles and power lines in the case of electricity) is covered by the charges to the consumer.[164]

113. There are three types of cloud services: public, private and hybrid. Under the public cloud model, a private sector company delivers the hardware, software and other network devices

---

[161] TBS, Guideline on Service and Digital, February 3, 2021, https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html.
[162] TBS, Guideline on Service and Digital, February 3, 2021, https://www.canada.ca/en/government/system/digital-government/guideline-service-digital.html; and TBS, "Designated Officials for Cyber Security (DOCS): #SecureGCDigital Forum," Presentation deck, February 25, 2021. The definition of an event is from TBS, Policy on Government Security, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578.
[163] TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html.
[164] TBS, Government of Canada Cloud Adoption Strategy: 2018 update, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html.

over the Internet. In this type of cloud, entities (including government organizations) rent space as "tenants" and share the same services and space with other organizations.[165] A private cloud consists of the delivery of the same services (hardware, software, network devices) on a private network used exclusively by one organization.[166] These services can also be delivered within the cloud tenant's physical premises. The hybrid approach is a combination of the public and private models. Notable service providers in Canada include Microsoft, with the Azure and Office 365 platforms, and Amazon Web Services.

114. Cloud services offer several benefits. One benefit can be streamlining costs, as organizations no longer manage or maintain the information technology assets included in the cloud environment (maintenance and management requirements are the responsibility of the cloud service provider). Another is that an organization's cloud requirements are scalable, meaning that they pay according to their changing computing requirements. TBS describes the benefits of public cloud services for the government:

- improved service performance due to scalable computing resources and contractually obligated performance levels;
- strong security as cloud service providers offer internationally recognized certifications that would be a challenge for a single organization to deliver;
- innovation through the deployment of new tools and technologies that are subscription based and do not require large capital investments; and
- greater flexibility in program development through a greater variety of resources and capacity offered in the cloud.[167]

Cloud environments are not devoid of risk, however. Government data stored in the cloud may still be subject to compromise or theft, and government operations that use cloud-based services may still be interrupted as a result of cyber threat activity. As with traditional computing environments, these require appropriate security controls to mitigate risks to privacy, data loss and service continuity.[168]

115. Since 2016, the government has pursued a cloud adoption strategy to maximize these benefits and mitigate risks. TBS notes that the adoption of cloud computing "will help the [government] maintain information technology service excellence during a period of increasing

---

[165] Microsoft, "What are public, private and hybrid clouds?," undated, https://azure.microsoft.com/en-ca/overview/what-are-private-public-hybrid-clouds/.
[166] Microsoft, "What are public, private and hybrid clouds?," undated, https://azure.microsoft.com/en-ca/overview/what-are-private-public-hybrid-clouds/.
[167] TBS, Government of Canada Cloud Adoption Strategy: 2018 update, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html.
[168] CCCS, Benefits and Risks of Adopting Cloud-Based Services in Your Organization (ITSE.50.060), March 2020, https://www.cyber.gc.ca/en/guidance/benefits-and-risks-adopting-cloud-based-services-your-organization-itse-50060; TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html, July 28, 2020.

demand for digital services and timely access to emerging technologies."[169] The strategy is also intended as a policy directive that emphasizes a number of requirements for federal organizations:

- a "cloud-first" adoption strategy in which cloud is the preferred option for delivering information technology services and public cloud is the preferred option for cloud deployment;
- an approach to managing security risks in cloud adoption that safeguards Canadians' data and privacy;
- a series of principles that will guide chief information officers as they adopt cloud services; and
- a vision for enabling community clouds, specifically, a Canadian public sector community cloud, to bring together Canadian public sector buyers with public cloud service providers, brokered and security-assessed by the Government of Canada.[170]

The strategy is aligned with Treasury Board direction included in the Directive on Service and Digital and the Digital Operations Strategic Plan. These documents also establish goals of enhanced service delivery through the use of cloud services, whereby departments must identify and evaluate them as a principal delivery option.[171]

116. Based on the requirements for departments to prioritize the use of cloud services, the CIO of Canada issued the Direction on the Secure Use of Commercial Cloud Services on November 1, 2017. This Directive ensures that security considerations are built into a department's approach through specific policy obligations.[172] For example, cloud environments can be used only for information holdings equal to or below a certain security category.[173] This direction is applicable to 110 federal organizations.[174]

117. In procuring cloud services, Shared Services Canada (SSC) functions as a broker for the government. This means that SSC contracts cloud service providers, accredits departmental

---

[169] TBS, Government of Canada Cloud Adoption Strategy: 2018 update, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html.

[170] TBS, Government of Canada Cloud Adoption Strategy: 2018 update, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html.

[171] See section 4.4.3.9, Directive on Service and Digital; and "Workload migration and cloud adoption," Digital Operations Strategic Plan 2018–2022.

[172] TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html.

[173] The government categorizes information by the expected type of injury should it be disclosed without authorization. The highest level of classification that may be used in the cloud is "Protected B," applied to information "when unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage." For information on other security categories, see TBS, Directive on Security Management – Appendix J: Standard on Security Categorization, July 1, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32614.

[174] The Direction on the Secure Use of Commercial Cloud Services is applicable to all departments within the meaning of Schedules I, I.1, II, IV and V of the FAA.

use and provides a self-service model that enables federal organizations to manage their cloud resources.[175] Nonetheless, departments (through their deputy heads) remain ultimately responsible for the management and safeguarding of their information, including in the cloud space, under the FAA. In accordance with the Direction on the Secure Use of Commercial Cloud Services, departments are therefore obliged to:

- apply graduated safeguards that are commensurate with identified risks;
- use third-party certification on the secure design of their cloud space;
- perform security assessments prior to receiving authorization for use;
- apply the separate direction for data residency, which requires departments to keep sensitive data in Canada;[176]
- manage vulnerabilities in information systems (e.g., through patching of vulnerabilities); and
- establish appropriate mechanisms to manage and respond to security incidents.[177]

To further support secure cloud implementation, a cloud operationalization framework (the cloud security guardrails) was established in 2019 to provide additional direction and guidance to departments. These guardrails reiterated the requirements outlined under the Direction on the Secure Use of Commercial Cloud Services, notably that TBS may disable a department's access to the cloud, should that department not meet these security requirements within 30 days of establishing a cloud environment.[178]

118. In short, the Cloud Adoption Strategy and the corresponding direction on secure use are meant to balance information technology enhancements with corresponding cyber security and cyber defence requirements.

---

[175] TBS, Government of Canada Cloud Adoption Strategy: 2018 update, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html; and TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html.

[176] The Direction for Electronic Data Residency IT Policy Implementation Notice directed departments and agencies on the control, access and ownership of government electronic data. The requirement to maintain "data residency" in Canada is meant to ensure continuous access to that data, afford data the protection of Canadian privacy laws, safeguard sensitive information in the interest of national security, and support more rapid responses in the event of a data compromise. TBS, Direction for Electronic Data Residency, IT Policy Implementation Notice (ITPIN), March 13, 2018, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html. This Notice was rescinded with the issuance of the Policy on Service and Digital and the corresponding Directive on Service and Digital, where the data residency requirement now resides.

[177] TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html.

[178] TBS, CIO of Canada, NSICOP appearance, November 27, 2020; TBS, "NSICOP Review – TBS Comments on Draft Final Report (9-July-2021)," pp.3, July 9, 2021; see also the Government of Canada Cloud Guardrails, part of the Cloud Operationalization Framework at https://github.com/canada-ca/cloud-guardrails.

Digital Operations Strategic Plan

119. The third foundational policy instrument for cyber defence is the Digital Operations Strategic Plan. Established in accordance with the Policy on Service and Digital, the Digital Operations Strategic Plan applies to 87 organizations.[179] Also consistent with the Policy on Service and Digital, the CIO of Canada must produce an annual forward-looking information technology plan for the whole of government. These strategic plans set the direction for departments on the priorities for the integrated management of services, information, data, information technology and cyber security. Between 2016 and 2019, the CIO of Canada published three such plans: the Government of Canada Information Technology Strategic Plan 2016–2020; the Government of Canada Strategic Plan for Information Management and Information Technology 2017–2021; and the current Digital Operations Strategic Plan 2018–2022. Due to the pandemic, the CIO of Canada did not prepare a plan in 2020, but intends to publish a version for the 2021–2024 period.

120. The 2018–2022 Digital Operations Strategic Plan builds on the two previous iterations. It restates the vision statement that "the Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device."[180] From a cyber defence and cyber security perspective, the plan mandates the development of an in-depth, layered approach that uses trusted (monitored) interconnection points that provide a gateway to cloud services. Overall, the strategy includes four broad categories of actions or initiatives that address key gaps or concerns for cyber defence and cyber security, all of which have varying completion timeframes within the strategic plan's timeframe.[181]

121. The first broad category aims to **bolster network consolidation, connectivity and perimeter security**. In pursuing the consolidation of network access to trusted external connection points, the government seeks to ensure the proper safeguarding of its information technology perimeter. As part of these efforts, SSC has reduced the number of internet connections. It will also complete network consolidation of the existing 50 SSC partner wide-area networks into a single enterprise network. Similarly, SSC will migrate 61 departments and agencies that do not currently use the SSC Enterprise Internet Service to the SSC-managed enterprise network (which use SSC Internet services exclusively and benefit from the protection of CSE's *** cyber defences) for a total of 104 departments by 2024.[182] As part of the Cloud

---

[179] As noted, the Policy on Service and Digital applies to organizations listed in schedules I, I.1 and II of the FAA.
[180] TBS, Digital Operations Strategic Plan 2018–2022, March 29, 2019, www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html.
[181] The next four paragraphs summarize key initiatives from the Digital Operations Strategic Plan. For more detailed information, see TBS, Digital Operations Strategic Plan 2018–2022, March 29, 2019, www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html. See also paragraphs 142 to 147 which detail additional information on Shared Services Canada cybersecurity projects, many of which support these initiatives.
[182] For more information on SSC's Enterprise Internet Service, see paragraphs 139 to 141 and 149 to 150. For additional information on SSC efforts to increase the number of departments using the service (the Small Departments and Agencies Project), see paragraph 151.

Adoption Strategy, the government will pursue the establishment of dedicated network connections to cloud service providers. This will ensure secure communications channels for government information. Moreover, TBS, CSE and SSC are establishing additional trusted interconnection points between government networks and external partners. Ultimately, these measures seek to consolidate the government's perimeter by narrowing external touch points to a limited number of trusted and secure connections.

122. The second broad category of initiatives seek to **secure endpoint devices**. Endpoint devices generally consist of laptops, desktops, smartphones, tablets and servers, or information technology assets used by government employees. In consultation with TBS and CSE, SSC will develop standardized procedures to securely configure endpoint operating systems and applications. This includes two key components: the deployment of an endpoint intrusion prevention system to automate the collection of information to identify malicious activity and prevent device compromise; and controls for accessing applications, which enable system administrators to identify and run permissible programs. Initiatives in this category will also support the deployment of tools and processes that monitor the real-time status and configuration of all endpoint devices (e.g., the status of hardware and software versions, operating system versions and patch installations). This capability will complement CSE's host-based sensors (see paragraphs 198–200), facilitate a comprehensive understanding of endpoint devices, and supplement the speed and ability of the government to address enterprise-wide vulnerabilities on endpoint devices. This initiative is expected to be completed in 2024.[183]

123. The third category of initiatives will **improve access control and application development**. These enhancements relate primarily to accounts for information technology systems administrators who have privileged access to departmental information technology systems. In 2019, TBS, SSC and departments strengthened the management and control of administrative privileges to minimize the misuse of any account with elevated privileges, and to ensure they are managed, controlled and monitored properly. In the future, TBS will improve secure application development by establishing an application security framework. Departments will apply this framework when developing and implementing digital services. The government's approach seeks to ensure that security is a key component of application design from the outset. This item is ongoing and does not have a scheduled completion date.

124. The fourth broad category aims to **improve awareness of cyber threats and risks to the government's systems and networks**. Similar to other actions within the Digital Operations Strategic Plan, this collection of initiatives seeks to improve the awareness of cyber risks and cyber threats through improved governance and training, while also bolstering the government's ability to respond to cyber incidents. In line with the above-noted enhancements for a centralized real-time view of endpoint devices, TBS proposes to establish a centralized capability to conduct governance, risk and compliance management activities. This will facilitate

---

[183] TBS, Government of Canada: Endpoint Visibility, Awareness and Security (EVAS) – Requirements (version 1.1), PDF. April 25, 2019; and TBS, Digital Operations Strategic Plan 2018–2022, March 29, 2019, www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html.

greater knowledge of the government's broad business technology environment that facilitates the identification of the system-wide attack surface and areas of vulnerability. TBS does not currently have a deliverable date for this project. Separately, TBS and CSE will develop a government vulnerabilities disclosure framework that quickly identifies and mitigates vulnerabilities. From a training perspective, the Canadian Centre for Cyber Security (CCCS) will promote a government-wide approach that enhances the cyber security of all employees. These efforts will help ensure that all system users contribute to system security and integrity. Lastly, TBS will update the Government of Canada Cyber Security Event Management Plan (see paragraphs 224–236), which describes the "stakeholders and actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely fashion."[184]

Summary

125. The Treasury Board and TBS play a central role in ensuring the proper administration and management of government. In the areas of cyber security and cyber defence, Treasury Board prescribes policies and directives that most (but not all) government organizations follow to ensure the integrity and security of their information technology assets and those of the government more generally. In turn, individual departments are ultimately responsible for ensuring their organization's cyber security and for safeguarding information and digital assets. Within this model of shared responsibility, SSC and CSE also play central roles in supporting departments to meet their obligations. The Committee discusses these organizations next.

Shared Services Canada

126. SSC is the second member of the Information Technology Security Tripartite. SSC is responsible for ensuring that the government's information technology infrastructure protects the government's technology assets and data in the government's possession.[185] This section discusses the evolution of SSC's mandate, key SSC services and projects to strengthen the government's general cyber security posture and those more specific to cyber defence, and SSC partners and clients.

SSC mandate

127. Prior to 2011, federal departments were viewed as unique in their individual information technology requirements. There was very little standardization as a result: departments were individually responsible for the acquisition and management of their information technology infrastructure, computers and devices, and for securing their electronic assets.[186] SSC was

---

[184] TBS, Government of Canada Cyber Security Event Management Plan 2019, July 28, 2020, https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.
[185] SSC, Cyber and Information Technology Security, undated, https://www.canada.ca/en/shared-services/corporate/cyber-information-technology-security.html.
[186] SSC, Serving Government: Remote Access Security Hardening Standard, undated, http://service.ssc-spc.gc.ca/en/policies_processes/policies/remote.

created in 2011 to fundamentally change this approach. The preamble to the *Shared Services Canada Act* (the SSC Act) establishes that the objective is to "standardize and consolidate, within a single shared services entity, certain administrative services that support government institutions; and doing so will enable those services to be provided more effectively and will support the efficient use of public money."[187] In practice, this meant consolidating the provision of email, data centre and network services to a core group of partner departments, and coordinating the purchase and provision of information technology equipment for the government.[188] While this consolidation was initially considered a cost-saving measure, the scope of the changes required necessitated considerable investments in following years.[189]

128. The authorities underpinning SSC have evolved. SSC was created by order in council in 2011. The department was then established in statute on June 29, 2012, when the SSC Act received Royal Assent. The SSC Act provides for a Minister to be designated as responsible for SSC – currently, the responsible minister is the Minister of State (Digital Government)[190] – and grants the Minister authority to coordinate telecommunications services for departments and agencies. SSC has the responsibility to:

- determine and deliver information technology solutions and common services across the government enterprise;
- plan and design forward-looking, consolidated and standardized services to meet the needs of partner and client departments;
- manage and maintain existing information technology infrastructure, including all necessary ongoing service and maintenance support;
- procure goods and services to enable the delivery of common information technology services to partner and client departments; and
- support government-wide information management and information technology security in partnership with CSE, including CCCS, and other government security partners.[191]

129. In total, the government has issued 21 orders in council to adjust SSC's mandate, appoint presidents of the organization, and expand the number of organizations to whom SSC must provide services or act to procure equipment and services.[192] Four of the orders in council are of particular relevance to this review:

---

[187] *Shared Services Canada Act*, S.C. 2012, C.19, S.711, Preamble, June 29, 2012, https://laws-lois.justice.gc.ca/eng/acts/S-8.9/page-1.html.

[188] Such as keyboards, desktop hardware and software, and monitors. Office of the Auditor General, *2015 Fall Reports of the Auditor General of Canada: Report 4—Information Technology Shared Services*, 2015, https://www.oag-bvg.gc.ca/internet/English/parl_oag_201602_04_e_41061.html.

[189] By 2020, investments in SSC alone totaled over $4 billion.

[190] Order in Council 2019-1366 designated the Minister of State (Digital Government) as the Minister for SSC. See https://orders-in-council.canada.ca/attachment.php?attach=38701&lang=en. From 2012 to 2019, the Minister of Public Works and Government Services was the responsible minister.

[191] SSC, "Shared Services Canada's Mandate, Authorities and Partners," Deck, Presentation to the NSICOP Secretariat. November 2020.

[192] SSC, "Shared Services Canada's Mandate, Authorities and Partners," Deck, Presentation to the NSICOP Secretariat, November 2020.

- In 2011, the government issued two orders in council that transferred six information technology-related units from then-Public Works and Government Services Canada,[193] and transferred the email, data centre and network services units of 42 departments to SSC, thereby creating SSC's 43 core "Partners."[194]
- In 2012, the government issued an order in council that circumscribed SSC mandate's by stipulating that it would not provide email, data centre or network services to any department that was accredited to process and store Top Secret information, or where four specified organizations used specific systems to operate ships, aircraft or vehicles or to support operations in the areas of national defence, national security or public safety.[195]
- In 2015, the government issued an order in council to expand the SSC mandate beyond its original 43 core partners to include 40 "Mandatory Clients" that would receive a subset of services related to email, data centres and network services on a cost-recovery basis. The order in council also expanded the number of government organizations required to procure end-user devices (e.g., desktop computers, printers) from SSC, and created a category of "Optional Clients" that could obtain services from SSC on a cost-recovery basis (the definition included Crown corporations and other levels of government).[196]

130. In sum, the periodic issuance of orders in council has established SSC's mandate and membership, and clarified its provision of services for email, data centres, networks and procurement for endpoint workplace technology devices. At present, SSC provides some or all services to 160 of 169 federal organizations (the Committee explores the issue of which departments are included later). See Table 1 for an overview of the division of responsibilities between SSC and individual departments.

---

[193] Order in Council 2011-0877, August 3, 2011, https://orders-in-council.canada.ca/attachment.php?attach=24554&lang=en.

[194] SSC is one of the 43 partners. Order in Council 2011-1297, November 15, 2011, https://orders-in-council.canada.ca/attachment.php?attach=24978&lang=en. This order in council resulted in SSC assuming responsibility for the information technology infrastructure of 42 partner organizations (servers, data centres, human resources and information technology budgets), including 485 data centres, 50 different networks and approximately 23,400 servers. This represented about 95 percent of the government's information technology infrastructure spending, with the remaining smaller departments and agencies representing the other 5 percent. SSC, Order in Council – Procurement, https://www.canada.ca/en/shared-services/corporate/transparency/briefing-documents/ministerial-briefing-book/order-in-council-procurement.html.

[195] The four organizations are the Canada Border Services Agency, the Department of Fisheries and Oceans, the Department of National Defence and the Royal Canadian Mounted Police. Order in Council 2012-0958, June 29, 2012, https://orders-in council.canada.ca/attachment.php?attach=26384&lang=en.

[196] Order in Council 2015-1071, July 16, 2015, https://orders-in-council.canada.ca/attachment.php?attach=31447&lang=en.

Government of Canada Information Technology Services			
Responsibility	Email, data centres, and networks	End-user devices	Applications
Service management and delivery	Shared Services Canada (mandatory or optional for specific departments as specified in orders in council)	Departments	
Procurement		Shared Services Canada	Public Services and Procurement Canada
Policy and standard setting	Treasury Board of Canada Secretariat		

Table 1: Distribution of Government of Canada Information Technology Service Responsibilities and Service Areas[197]

SSC services and projects

131. SSC has a fundamental role in ensuring that government digital assets and information are protected. Its provision of email, networking and data centre services means that it provides the infrastructure that houses and carries important information belonging to Canadians and to the government. This infrastructure supports the delivery of government programs, and Canadians expect and depend on consistent and reliable service from those programs. The persistent threat of cyber attack against this infrastructure means that cyber security remains a significant risk; where technical or operational security controls are inadequate, or where security vulnerabilities are not addressed, government systems remain vulnerable to malicious cyber activity.[198] As SSC notes, the security of the government's information technology infrastructure is therefore of "paramount importance."[199]

132. The Committee understands SSC's fulfillment of its responsibilities as falling into two broad categories. The first is the ongoing protection of government digital assets and communications through the proper management of information technologies (SSC services). The second is the implementation of a government-wide information technology infrastructure plan to better protect government systems against security threats (SSC projects).[200] The Committee discusses each of these in turn.

Cyber defence and SSC services

133. The networks and data that SSC is responsible to protect vary widely in size, function and mandate. These differences are representative of the variability in government programs and service delivery. Some organizations hold little sensitive information on their networks and therefore face relatively few security threats; others hold large amounts of sensitive information

---

[197] Adapted from: SSC, Shared Services Canada History and Legislative Responsibilities, February 3, 2016. https://www.canada.ca/en/shared-services/corporate/transparency/briefing-documents/ministerial-briefing-book/shared-services-canada-history-legislative-responsibilities.html; and SSC, "Shared Services Canada's Mandate, Authorities and Partners," Deck presented to NSICOP Secretariat, November 2020.

[198] The Departmental Security Plan identified two other significant security risks: the security of the SSC workforce, workplace, facilities and assets; and the governance of SSC security-related activities. SSC, Departmental Security Plan 2019–2022, May 15, 2019. Similar risks were also identified in SSC's 2013–2016 Departmental Security Plan.

[199] SSC, Departmental Security Plan 2019–2022, May 15, 2019; and SSC, Shared Services Canada Network and Security Strategy (version 1.6), September 1, 2020.

[200] SSC, "Mandate," https://www.canada.ca/en/shared-services/corporate/mandate.html.

and face significantly greater threats.[201] To respond to these threats, SSC applies a number of cyber security measures to identify and prevent malicious actors from gaining access to government networks, including firewalls, anti-virus and anti-malware services, and identification and authentication tools.[202] SSC is responsible for the government's Secret-level network infrastructure, and collaborates with CCCS to manage the government's network perimeter by using specialized security monitoring of Internet gateways (see the section, "The Communications Security Establishment") that have enhanced the government's ability to detect and deter malicious cyber activity.[203] All together, SSC offers 34 different services to its partners and clients that fall across five categories, and contain at least one service of relevance to SSC's role in defending government networks from cyber attack. The following paragraphs briefly describe each of the services and their relevance to cyber defence.

Digital services

134. Digital services is the largest category of services provided by SSC. Of the 12 services in this area, four play a role in cyber defence. The first two are the provision of email accounts for government employees and the means of accessing them remotely through secure network connections. These two services are subject to user identity and credential management controls, and monitored for viruses and spam. The third service is the provision of mobile devices (cell phones) for telephony, email and Internet connectivity.[204] The fourth service is an identity validation system for ensuring synchronized, system-wide control and management of user credentials, to provide access to government systems and information in both cloud environments and standard, "on premises" networks.[205]

Security services

135. SSC security services authenticate individuals to access government services and accounts, both internally and externally to government networks. Three elements in this service area are relevant to defending government networks:

- **Internal credential management:** SSC manages a public key infrastructure that facilitates authentication for secure access to applications and government networks.[206]

---

[201] SSC, Departmental Security Plan 2013-2016, June 17, 2013.
[202] SSC, "Cyber and Information Technology Security", https://www.canada.ca/en/shared-services/corporate/cyber-information-technology-security.html.
[203] TBS, Government of Canada Cyber Security Event Management Plan (CSEMP), 2019, https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html#toc6; Public Safety Canada, Horizontal Evaluation of Canada's Cyber Security Strategy, September 29, 2017, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-en.aspx#s331.
[204] SSC, "Serving Government: Email – for Administrators," http://service.ssc-spc.gc.ca/en/services/communicating/email/admin; and SSC, "Serving Government: Mobile Devices – for Government of Canada Employees," http://service.ssc-spc.gc.ca/en/services/communicating/mobile-dev-phones/mobile-users.
[205] SSC, "Serving Government: Service Catalogue," http://service.ssc-spc.gc.ca/en/services; and SSC, Directory Credential and Access Management. Implementation Business Case (version 3.0), September 8, 2020.
[206] A public key infrastructure is used to protect the confidentiality of information and to electronically authenticate the identity of individuals in accessing protected information. TBS, *Guideline on the Management of Public Key Infrastructure in the Government of Canada*, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=20008#appB.

The service allows users to exchange encrypted email up to a certain classification and to securely access applications that process sensitive personal information (e.g., pay information).[207]

- **Secure remote access management:** This service uses the public key infrastructure (above) to permit users to securely transmit and receive information from remote workstations while maintaining the availability, confidentiality and integrity of data.[208]
- **External credential management:** SSC manages a public key infrastructure that provides a standardized cyber authentication service to Canadians, businesses and individuals to permit secure online business with various governmental programs and services.[209] This service is mandatory for departments and agencies.[210]

Hardware and software services

136. SSC provides departments with procurement options for devices such as computers and printing equipment, and for multiple kinds of software, including for connectivity, individual devices and security needs. Services of relevance to cyber defence include:

- **Hardware provisioning and procurement:** SSC procures workplace technology devices (hardware) for its partners and clients, including desktop computers, laptops and tablets.[211]
- **Software provisioning and procurement:** SSC procures software for its partners and clients for devices (e.g., device operating systems), services (e.g., desktop software configuration), connectivity (e.g., print services), productivity (e.g., web browsers) and security (e.g., user authentication).[212]

137. All SSC hardware and software procurement services are subject to the SSC Supply Chain Integrity Standard. This standard is meant to identify and assess any procurement process that "could be compromised, or used to compromise, the security of Canada's [hardware], software, services or information," and to ensure that hardware and software identified for procurement is subject to a security assessment (including engagement with CSE), contracts are audited, and that items identified as high risk can be avoided, recalled, or removed from government systems.[213]

---

[207] SSC, "Serving Government: MyKey – For Government of Canada Employees," https://service.ssc-spc.gc.ca/en/services/access/mykey/users.
[208] SSC, "Serving Government: Secure Remote Access – For Administrators," https://service.ssc-spc.gc.ca/en/services/access/secure-remote-access/admin.
[209] SSC, "Serving Government: Service Catalogue," https://service.ssc-spc.gc.ca/en/services, and SSC, "Serving Government: Responsibilities Matrix for Cyber and IT Security. Section 6.0 Identity and Access Management (IAM) Services," http://service.ssc-spc.gc.ca/en/itsecurity/RACI#securitystandards1.2.
[210] SSC, "Serving Government: Service Catalogue," https://service.ssc-spc.gc.ca/en/services.
[211] SSC, "Serving Government: Microcomputers," https://service.ssc-spc.gc.ca/en/services/hw-sw/microcomputers/procure; and SSC, Shared Services Canada, Supply Chain Integrity Standard, November 2015.
[212] SSC, "Serving Government: Software – For Procurement," https://service.ssc-spc.gc.ca/en/services/hw-sw/software-provisioning/procurement.
[213] SSC, Shared Services Canada Supply Chain Integrity Standard, November 2015.

Data centre services

138. SSC offers nine data centre services. While these are predominantly database infrastructure and hosting services, this service includes two important elements for cyber defence:

- **Cloud Brokerage Services:** Consistent with the 2017 Treasury Board Direction on the Secure Use of Commercial Cloud Services, SSC provides a brokerage service for government departments to identify suitable cloud service providers with whom SSC has established contracts. SSC provides this service to all 43 partners, 23 SSC mandatory clients and 15 optional clients.[214]
- **Government of Canada Secret Infrastructure:** SSC manages and maintains this Infrastructure to permit the creation, processing, storage and sharing of information classified at the Secret level. The service uses the government's wide area network for transmission of encrypted data between users and departments. Risks in protecting more sensitive information at the Secret level are shared between SSC and customer departments or agencies, with SSC responsible for maintaining the integrity, assurance and effectiveness of security controls for approved users, and departments responsible for managing user access to their applications and data.[215]

Network services

139. SSC networking services include the provision of wi-fi, Internet services and satellite connectivity. There are eight elements within network services, with the following two of critical importance to the government's framework for cyber defence:

- **The Government of Canada Wide Area Network (GC WAN):** The GC WAN is a fully managed network service that connects partner or client locations across metropolitan, regional, national or international boundaries. It connects users and computers to each other and the Internet, and it supports simultaneous voice, data and video communications, and the transmission of classified information using appropriate encryption. The GC WAN services come with security monitoring and enhanced security protocols (e.g., logging and intrusion detection services).[216]
- **Enterprise Internet Service:** The SSC Enterprise Internet Service provides secure connectivity for government users to access the Internet and for the public to access

---

[214] SSC, "Serving Government: Cloud Brokering Service," https://service.ssc-spc.gc.ca/en/services/dc/cloud; TBS, Government of Canada Cloud Adoption Strategy: 2018 Update, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html; and TBS, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html.

[215] SSC, "Serving Government: Government of Canada Secret Infrastructure Network and Hosting – for Administrators," http://service.ssc-spc.gc.ca/en/services/infrastructure/classified/gcsi. In the past, the government maintained 34 stand-alone, independently managed Secret-level networks across 18 departments. The GCSI Expansion Project includes efforts to transition those networks to SSC enterprise architecture for one system for secret communications and data. See also, SSC, *Secret Infrastructure. 34 Legacy Networks,* undated.

[216] SSC, "Serving Government: GC WAN – For Administrators," http://service.ssc-spc.gc.ca/en/services/infrastructure/network-infra/gcnetwan-admin.

> government websites. SSC provides the Enterprise Internet Service to all of its partner organizations and on a fee-for-service subscription basis for its clients. The service requires a GC WAN connection and provides the highest protection, owing to built-in security monitoring and enhanced security protocols provided by the integration of CSE's *** cyber defences to Enterprise Internet Service Internet gateways. The Committee further explores the benefit of this integration in the discussion of CSE below.[217]

Overall, the creation of SSC's Enterprise Internet Service and its progressive adoption by departments has played a foundational role in strengthening the government's cyber defence framework. Its evolution is described below.

Secure Internet connectivity: The evolution toward the Enterprise Internet Service

140. The origins of SSC's Enterprise Internet Service date to 2002 when the government launched the Secure Channel Network as a means for federal organizations to securely deliver their most commonly used services online.[218] The Secure Channel Network was intended to reduce operational and maintenance costs through the use of a common network infrastructure for government that included monitored, protected and redundant access to the Internet.[219] In 2006, Treasury Board provided direction to make the use of the Secure Channel Network mandatory and by 2008, 75 departments had migrated to it. In 2010 and 2011, China conducted large-scale attacks against numerous government departments, resulting in the loss of significant amounts of sensitive data (see case study 1). In response, the Chief Information Officer of Canada again issued directives to require departments to migrate to the Secure Channel Network to:

> reduce the risks we are currently collectively facing from ever increasing external cyber attacks. The key approach for mitigating these risks is to reduce the number of individual departmental Internet connections and replace these with a robust, high-performing and very secure common access for [government]. Decreasing the number of Internet access points – and securing those points – will reduce the overall [information technology] security risk to the Government, making it easier to prevent and defend against attacks aimed at disrupting our business or stealing sensitive and private information.[220]

By 2012, the number of departments using the Secure Channel Network grew from 75 to 87.[221]

---

[217] SSC, "Serving Government: Service Catalogue," http://service.ssc-spc.gc.ca/en/services. Also SSC, "Serving Government: GC WAN – For Administrators," http://service.ssc-spc.gc.ca/en/services/infrastructure/network-infra/gcnetwan-admin.
[218] SSC, Discussion on mandate with NSICOP Secretariat – February 24 and follow-ups, March 9, 2021.
[219] SSC, Discussion on mandate with NSICOP Secretariat – February 24 and follow-ups, March 9, 2021.
[220] SSC, "SCNet Enterprise Internet – 2010 and 2011," TBS CIOB communique, February 24, 2021.
[221] SSC, Discussion on Mandate with NSICOP Secretariat – Feb 24 and follow ups, March 9, 2021.

141. In 2015, the Secure Channel Network became the Enterprise Internet Service and the number of departments using it grew to 90. All SSC core partners have moved to the Enterprise Internet Service (with the exception of the Department of National Defence, which will be migrated in 2021–2022), as have a number of SSC's mandatory clients and optional clients.[222] However, government-wide adoption of the Enterprise Internet Service remains a challenge. In 2018, Treasury Board reiterated its direction to government departments to migrate to the Enterprise Internet Service:

> To address risks to its network, the government is standardizing protection and creating a secure, government-wide perimeter that will protect government data both on premises and in the cloud. TBS, the Communications Security Establishment (CSE) and SSC are establishing additional trusted interconnection points between the government [backbone] network and external partners to: provide standardized and secure connectivity with external partners and the Internet; act as a gateway to cloud services; and protect cloud-based workloads from direct attacks from the Internet. Departments that do not currently use SSC Internet services will be migrated to the SSC-managed enterprise network and will use SSC Internet services exclusively.[223]

Requiring this migration makes sense. As discussed in further detail in the section on the CSE (paragraphs 154–213), CSE and SSC manage a highly effective system of sensors and defence tools (both classified and commercially available) that protect government organizations within the Enterprise Internet Service from normal threats and, most importantly, the most sophisticated cyber threat actors. As of August 2021, SSC provides the Enterprise Internet Service to 94 organizations.[224] The Committee addresses the issue of Treasury Board direction and the number of departments using SSC's Enterprise Internet Service in its assessment.

---

[222] SSC, Discussion on Mandate with NSICOP Secretariat – Feb 24 and follow ups, March 9, 2021. The Department of National Defence *** is monitored separately by CCCS.
[223] TBS, Digital Operations Strategic Plan 2018–2022, Section 4.2, "Secure the government's evolving perimeter," https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html
[224] SSC, NSICOP Discussion on Mandate with Committee Secretariat – Feb 24 and follow ups, Email, March 9, 2021; and SSC, "Re: NSICOP Discussion on Mandate with Committee Secretariat," Email, April 30, 2021.

Case study 1: A wake-up call - network consolidation and dynamic defences

[*** Four paragraphs were revised to remove injurious or privileged information. ***] In February 2010, CSE deployed its sensors to the government's Secure Channel Network, the first time CSE had used this capability outside of three departments: Foreign Affairs and International Trade (now Global Affairs Canada), National Defence, and CSE itself.[225] CSE immediately discovered a long-standing and significant compromise of government networks by a Chinese state-sponsored actor. The Chinese actor was known to target government networks around the world for intelligence related to natural resources and energy, defence, global finances, foreign policy, and trade. CSE assessed that the actor sought to acquire Canadian position papers, briefing notes and strategies for multilateral negotiations related to several international bodies.

Between August 2010 and August 2011, China targeted 31 departments, with 8 suffering severe compromises. Information losses were considerable, including email communications of senior government officials; mass exfiltration of information from several departments, including briefing notes, strategy documents and Secret information; and password and file system data. Treasury Board of Canada Secretariat and the Department of Finance were the worst affected, losing entire sets of network passwords.

CSE launched a three-pronged response. First, it monitored malicious activity through its network sensors. Second, it provided advice and guidance to departments to improve system management and security. Third, it aided in the strategic mitigation of the compromise, using its information to better understand the attacker's intentions and capabilities. For their part, Treasury Board of Canada Secretariat and the Department of Finance were forced to disconnect their networks from the Internet to mitigate the compromise.

This incident was a wakeup call for the government regarding the scale of its cyber vulnerability and the need for commensurate defences. To that point, government networks were an easy and valuable target for Chinese state-sponsored threat actors, as they were essentially undefended and used to store classified information in the absence of a secure alternative. The deployment of CSE's network-based sensors to this broad network was a "turning point in the history of Cyber Defence in the government" – it confirmed the need for consolidated Internet access points that could be monitored for threats and for a single, government-wide enterprise network to properly secure government systems from cyber attack.[226]

---

[225] This summary is based on CSE, Analysis of Widespread Chinese Intrusions on Government of Canada Networks, April 2010; CSE, Interdepartmental Assessment: The Chinese Cyber Threat to Government of Canada Networks – August 2010–August 2011, undated; CSE, "DM Security and Intelligence: Update on January 2011 Cyber Intrusions," Memorandum for the Chief, CSE, February 2011; and CSE, NSICOP Cyber Defence Review – Information Package #17 – Table of Contents, March 11, 2021.

[226] CSE, NSICOP Cyber Defence Review – Information Package #17 – Table of Contents, p. 1, March 11, 2021.

Cyber defence and SSC projects

142. The second broad category of SSC responsibilities is the implementation of a government-wide information technology infrastructure plan to better protect government systems against security threats, that is, SSC projects. SSC uses a secure-by-design approach to integrate its cyber security activities into its core responsibilities.[227] This means that SSC services and activities are designed and built to incorporate applicable engineering and security standards, and to comply with government security policies. In practice, this means that SSC maintains its own internal security policy instruments, each one a guide for consistently implementing an information technology security standard.[228] SSC currently has 12 active cyber security projects, organized into three areas: identity and access control, connectivity, and monitoring. These areas and their relevance to cyber defence are described below.

Identity and access control

143. Verifying a user's identity and controlling the user's access to required elements of a department's digital infrastructure is essential to ensuring the security of digital systems.[229] Identity and access controls are meant to ensure that users are authorized to access only the digital resources they require, consistent with their role in an organization. In the past, the government used a castle-and-moat approach, where the focus was securing the perimeter of the network, authenticating and granting access to approved users at secure entry-points, and layering defensive systems (e.g., firewalls) to filter network access. SSC described it as "a defence in-depth posture that uses a series of defensive mechanisms layered to protect valuable data and information. If one mechanism fails, another steps up immediately to thwart an attack."[230]

144. SSC notes that this approach is increasingly unviable in a digital environment marked by the proliferation of devices and connection options and greater user mobility requirements. It is therefore implementing several projects to modernize identity and access control. These will build on effective perimeter defences to include continuous verification and authorization of users and devices. The most important are as follows:

- **Network Device Authentication:** Network device authentication is meant to improve the authentication of devices to government networks (as opposed to individual users and their accounts). The project aims to improve access controls, auditing functions and forensic analysis of devices accessing a network, the latter a significant gap in responding to compromises of government systems.[231]

---

[227] SSC, Departmental Security Plan 2019–2022, May 15, 2019.
[228] The 16 SSC information technology security standards cover multiple areas, including management of security systems logs, supply chain integrity, perimeter security, patch management for servers and workstations, and network and Internet access. SSC's information technology security standards are available at http://service.ssc-spc.gc.ca/en/policies_processes/policies.
[229] SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020.
[230] SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020.
[231] During cyber attacks, officials often spend significant time analyzing forensic data to differentiate between legitimate network activity and activity attributable to malicious cyber actors.

- **Secure Remote Access Modernization:** Secure remote access to government networks is currently done at the individual department level. This project is designed to migrate secure remote access to a consolidated government-wide enterprise system. The project will improve cyber defence functions related to remote connectivity, including connectivity logs, analytics regarding threat detection and traffic volume management.[232]
- **Administrative Access Controls Service:** Network administrators tend to share and re-use passwords, reducing barriers to cyber attackers' ability to gaining broad access to multiple networks within and across departments. The project is meant to eliminate this practice by standardizing and enforcing the management of administrative privileges.[233]
- **Directory Credential Account Management:** This project is designed to enable greater collaboration by SSC partners and clients in cloud operating environments by synchronizing user credentials through a centralized user authentication service in the cloud. It will allow SSC to authenticate a user's identity between cloud and non-cloud workspaces.[234]
- **Internal Centralized Authentication Service:** This project will provide government-wide, standardized credentials (e.g., usernames and passwords) and a centralized authentication service to support web-based access to internal applications regardless of organization. It will enable the transition to more robust security credential technology and the retirement of browser technologies with security vulnerabilities.[235]

Connectivity

145. Managing digital connectivity for government users and systems is an important challenge for cyber defence. The current government network is a complex mixture of telecommunications connectivity to approximately 4,000 locations, 5,000 buildings and hundreds of thousands of fixed and mobile digital devices for government employees and contractors in Canada and abroad.[236] Historically, government departments operated more than 720 data centres across Canada, all without shared infrastructure, standards for network configurations or connectivity, operating procedures, or standardized service levels for redundancy and availability.[237] To address the many challenges that this situation poses, SSC intends to consolidate legacy data centres into four regional hubs, implementing a wireless-first approach for intra-building connectivity, and adopting new technologies (e.g., the adoption of 5G and the expanded use of mobile technology).[238] This evolution of SSC connectivity measures

---

[232] SSC, Shared Services Canada: Network and Security Strategy. (version 1.6), September 1, 2020.
[233] SSC, Administrative Access Control Services. Project Proposal (version 1.7), September 12, 2016. PDF. This project responds to the Auditor General's Fall 2015 report on information technology shared services in the Government of Canada.
[234] SSC, Directory Credential Account Management (DCAM) – DCAM Overview (version 1.7), December 5, 2019. PDF.
[235] SSC, Internal Centralized Authentication Service (ICAS): Concept of Operations (Con-Ops) (version 1.1), October 8, 2020.
[236] This includes government departments in single and multi-tenant buildings in multiple locations across Canada, using hard-wired infrastructure, wireless connectivity, and varied approaches to technology deployment, maintenance, and contracting with vendors and telecommunications service providers.
[237] SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020.
[238] SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020.

will require commensurate security measures to protect networks, data centres and their users. SSC connectivity projects in this area include the following:

- **Enterprise Perimeter Security:** This project is designed to provide enhanced visibility of cyber threats targeting government networks and their connections to departmental cloud environments. By leveraging the identity and access control projects, this project enables secure remote connectivity to government networks, from any location, including through physical or virtual connection links. This project will also provide additional visibility on cyber threats to both SSC and CCCS.[239]
- **Secure Cloud Enablement and Defence:** This project will provide the connectivity and security controls (controlled, monitored gateways) necessary for government departments to access and safeguard sensitive information in cloud networks. This will include centralized logging and monitoring to permit identification and management of security events affecting cloud-based data, and of threats to government networks that may originate from a cloud environment and target the government backbone network. Similar to the Enterprise Perimeter Security project, this project will provide additional visibility on cyber threats to both SSC and CCCS.[240]
- **Secret Infrastructure Expansion:** SSC maintains a dedicated infrastructure to store and transmit information classified as Secret. Currently providing service to 31 departments, this project will expand SSC's current infrastructure to some new clients and expand services to a number of existing clients.[241] This will fill a considerable gap – in the past, some departments handled Secret information on unclassified networks, resulting in the loss of classified information to state actors.[242]
- **SmartPhone for Classified:** Some government officials require an ability to securely communicate by phone and mobile data to support operations. This project will build on a CSE proof of concept to provide an initial capacity of 2,000 government users across Canada and to select international locations, with scalability up to 10,000 users.[243]

Monitoring

146. Security monitoring of the government's information technology infrastructure ensures its consistent and reliable performance, and supports the government's business continuity and provision of services to Canadians. Monitoring activities include the identification of events

---

[239] SSC, "Networks, Security, and Digital Services and the Senior Assistance Deputy Minister, Project Management and Delivery. For Decision. Enterprise Perimeter Security (EPS) Authority to Operate (ATO)," Memorandum to the Authorizing Official and Senior Assistant Deputy Minister, undated; and SSC, *Enterprise Perimeter Security (EPS)*, Security Assessment Report, April 7, 2020.

[240] SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020; and SSC, "SSC Networks, Security and Digital Services: Cyber and IT Security Program," Presentation to the Canada Revenue Agency (CRA), February 4, 2020.

[241] SSC, "Government of Canada Secret Infrastructure Expansion (GCSI Expansion)," Implementation Business Case (version 2.2), September 28, 2020; SSC, Government of Canada Classified (SECRET) Information Technology Convergence Update, April 8, 2020; SSC, Government of Canada Secret Infrastructure Expansion (GCSI Expansion), Project Management Plan, September 28, 2020; and SSC, Secret Infrastructure: 34 Legacy Networks, undated.

[242] See case study 1.

[243] SSC, "SmartPhone for Classified," Implementation Business Case (version 0.13), October 19, 2020.

related to user identification and authentication on a network or device, the monitoring of network traffic transiting a government communications link and the use of applications on end-user devices. When done well, proactive monitoring enables administrators to rapidly identify and address security events on network devices. That is not currently the case. Security monitoring of government networks is inconsistent, with networks variously monitored by SSC, SSC core partners and organizations that have no relationship with SSC. Moreover, SSC's own security information and event management system is not standardized for all of its clients.[244] Overall, this means that SSC does not have full visibility over government networks to identify risks and to respond to incidents quickly, resulting in inconsistent accountability for network monitoring across government.[245]

147. Building on the consolidation of government data centres, SSC is implementing three projects to centralize its security monitoring to broaden its awareness of activities on government networks and to enable more rapid and coordinated incident response capabilities.[246] These projects are:

- improving SSC's real-time situational awareness of the security posture of endpoint devices (e.g., laptops, desktops, tablets and servers);[247]
- improving SSC's awareness of security vulnerabilities across larger elements of the government's information technology enterprise (e.g., within data centres);[248] and
- monitoring network communications for events that may indicate a potential security incident and to notify SSC users to take remedial action to investigate and respond where necessary.[249]

Across all three projects, SSC is focusing on automating the monitoring of deployed devices and network connections and assessing their security posture against known vulnerabilities or emerging cyber threats. Each project is designed to improve SSC situational awareness and to fill identified gaps in government network security (e.g., lack of awareness regarding up-to-date patching for security vulnerabilities). In the event of a serious cyber incident, the projects are

---

[244] While SSC provides the electronic platform for security information and event management, CCCS is responsible for its configuration and operation, and the monitoring of events.
[245] SSC, Shared Services Canada: Network and Security Strategy, (version 1.6), September 1, 2020. Of note, departments also have key responsibilities in monitoring and securing their networks and endpoints (see paragraphs 102 to 105).
[246] SSC, Shared Services Canada: Network and Security Strategy, (version 1.6), September 1, 2020.
[247] SSC, Endpoint Visibility Awareness and Security Project. Project Management Plan, (version 1.0), March 30, 2020. See also SSC, "SSC Networks, Security and Digital Services: Cyber and IT Security Program," Presentation to CRA, February 4, 2020. At full implementation, the project will provide automated information on as many as 900,000 endpoints across government networks, consolidating individual department snapshots into a government-wide status.
[248] The Enterprise Vulnerability and Compliance Management project, noted in SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020.
[249] The Security Information and Event Management project. SSC, "Security Information and Event Management," Business Case (version 1.1), November 6, 2018; SSC, "SSC Networks, Security and Digital Services: Cyber and IT Security Program," Presentation to CRA, February 4, 2020. See also SSC, Shared Services Canada: Network and Security Strategy (version 1.6), September 1, 2020. Of note, CCCS is now responsible for this project.

meant to enhance the capacity to assess, in real time, points of weakness in the enterprise network and to reduce the time required to detect, respond and recover from a cyber incident.

SSC partners and clients

148. SSC provides services to the following three categories of departments or agencies. The categories determine the types of services provided, the latitude specific organizations have in determining which SSC services they will use, and how costs for services are attributed:

- **Core partners:** Since 2011, SSC has been responsible for managing the network infrastructure for 43 partner departments and agencies. At the time, these organizations transferred their respective budgets and personnel for email, data centres and network services to SSC, and consequently received all SSC's services without additional cost.
- **Mandatory clients:** In 2015, the SSC mandate was expanded to include mandatory clients. These organizations, which include small departments and agencies, must use certain SSC services in areas of email, data centres, networks and endpoint devices, or to procure other digital infrastructure. There are currently 39 mandatory clients, which pay SSC for services on a cost-recovery basis.[250]
- **Optional clients:** In 2015, SSC's mandate was expanded to include optional clients. Optional clients may request SSC services on a cost-recovery basis, and could include a provincial government or municipality, Canadian aid agency, public health organization, intergovernmental organization or a foreign government. There are currently 78 optional clients.[251]

Currently, SSC provides all or some of its services to 160 of 169 federal government organizations.

149. Which organizations are included as part of SSC's service delivery has significant implications for the government's cyber defence framework. As SSC evolved, it implemented increasingly comprehensive measures to protect digital infrastructures (e.g., the reduction of Internet connection points, the introduction of CSE's advanced sensors and defences on SSC Internet gateways) and, through its projects to modernize government digital infrastructure, developed a secure-by-design approach to email, data centre and network solutions.[252] While this evolution involved significant challenges for SSC and partner organizations, these benefits

---

[250] SSC, "Improve the Internet Security Posture of Small Departments and Agencies," Business case, December 15, 2020. There were 40 clients in 2015. See also SSC, "Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20," Deck, Provided to NSICOP Secretariat March 24, 2021.

[251] SSC, "Serving Government: Order in Council 2015-1071 Questions and Answers," http://service.ssc-spc.gc.ca/en/policies_processes/oic2015-1071-qa. SSC currently provides a public key infrastructure service to two organizations, the office of a minister of the British Columbia government and the Ontario Provincial Police, and the GC WAN service to the Government of Ontario.

[252] SSC, "Re: NSICOP Discussion on Mandate with Committee Secretariat," Email, May 21, 2021.

have come automatically to SSC's 43 core partners through their status as organizations that receive all SSC services.[253]

150. That is not the case for SSC's mandatory and optional clients. These clients vary significantly in terms of size, mandate, complexity, the modernity of their digital infrastructure, and their budget for digital technology and security.[254] Some of the organizations obtain SSC services through links with SSC core partners;[255] others use only a selection of SSC services; some obtain a mix of information technology services from SSC and private service providers; and others do not connect to a government network at all.[256] Many of these organizations are known as small departments and agencies, defined as having fewer than 500 staff and an annual budget of less than $300 million. These departments and agencies pose a security risk to government networks for three reasons:

- they may lack connectivity to the secure Internet gateways provided by SSC and to SSC-brokered secure cloud access. In such cases, these departments and agencies would not receive the advanced cyber monitoring of CCCS;
- they employ varied services for Internet connectivity, often from multiple physical locations, and maintain connectivity to other government departments; and
- they have limited resources (personnel or financial) to address Internet security issues, resulting in inconsistent cyber defences.[257]

Notably, SSC identified four departments and agencies that posed high or critical risks to government networks because of their simultaneous connections to government networks and use of third-party Internet connections that had few or no defensive measures.[258] In short, these organizations hold government data and often have electronic links into government departments, but do not necessarily benefit from SSC's (and CSE's) range of cyber defence measures, nor SSC's secure-by-design projects to modernize the government's digital infrastructure. (This is also true for mandatory clients that do not use SSC's Enterprise Internet Service.) As a result, cyber attacks against those organizations (including the loss of data) may

---

[253] SSC noted that it inherited many disparate systems from its partner departments and that the effort to design and implement an enterprise security approach for all of its partners has been an iterative one. SSC, Addendum to the Business Case for the Small Departments and Agencies Study, November 30, 2020. Some departments, like the Royal Canadian Mounted Police, struggled to have their unique operational requirements recognized by SSC.
[254] SSC, "Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20," Deck, Provided to NSICOP Secretariat March 24, 2021.
[255] Eight organizations, including the National Farm Product Council (under Agriculture and Agri-Food Canada); the Veterans Appeal and Review Board (under Veterans Affairs Canada); the Canada Employment Insurance Commission (under Employment and Social Development Canada); the Department of Indigenous Services (under Crown-Indigenous Relations and Northern Affairs Canada); the Parole Board of Canada (under the Correctional Service of Canada); the Office of the Correctional Investigator of Canada (under the Correctional Service of Canada); the Leaders Debates Commission (under the Privy Council Office); and the Copyright Board (under Innovation, Science and Economic Development Canada). SSC, "Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20," Deck, March 24, 2021.
[256] SSC, "Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20," Deck, March 24, 2021.
[257] SSC, "Improve the Internet Security Posture of Small Departments and Agencies," Business case, December 15, 2020.
[258] SSC, *Improving the Internet Security Posture of Small Departments and Agencies Study: Survey Report* (version 1.0), December 15, 2020.

go undetected, and the government may be unable to respond effectively or at all to significant cyber incidents. The inability of these organizations to adequately protect themselves is a risk to their own digital infrastructure and potentially to other government organizations.

151. In 2020, Shared Services Canada (SSC) developed a four-year project to address the challenge of organizations being connected to Government of Canada networks without being required to install robust cyber defences or being subject to oversight by SSC or CCCS. The Small Departments and Agencies Project aims to raise all small departments and agencies and mandatory clients (61 in total) to maximum SSC network security levels by providing them with access to the government backbone network (GC WAN), full network security at the same level as an SSC core partner, monitoring by CCCS and SSC enactment of all the network security improvements.[259]

The primary objectives of the project are to:

- bring all mandatory clients and small departments and agencies "inside the security fence" so that they use SSC secure Internet gateways, which would reduce the number of external connections to departmental networks;
- consolidate Internet connection points through SSC's regional communications hubs, which would improve visibility of network traffic to SSC and CCCS and allow SSC and CCCS to apply higher-level cyber defences for identifying and mitigating unauthorized entry, data exfiltration and other malicious activity; and
- increase the cyber security posture of government through the elimination of different classes of network security for SSC partners and mandatory clients.[260]

Notwithstanding the importance of this initiative, it currently has neither a budget nor a timeline for implementation.[261]

Cyber security event management

152. As part of its broad responsibilities, SSC coordinates with its partners to respond to serious cyber incidents. SSC is responsible for:

- blocking cyber threat activities from targeting SSC-managed networks and mitigating their effects;
- responding to CCCS recommendations and ensuring that updates and mitigating measures are applied in a timely manner;
- implementing prevention, mitigation and recovery efforts (among other things, this could include shutting down or isolating specific networks);

---

[259] SSC, "Improve the Internet Security Posture of Small Departments and Agencies," Business case, December 15, 2020.
[260] SSC, "Improve the Internet Security Posture of Small Departments and Agencies, Business case," December 15, 2020.
[261] SSC, "SSC Comments," email to NSICOP Secretariat, July 28, 2021.

- supporting the identification, risk assessment, mitigation, recovery and post-analysis of cyber security events within the government;
- assessing government-wide impacts of cyber security events, threats and vulnerabilities on program and service delivery; and
- producing post-event reports, including a timeline of events and root-cause analysis, to be submitted to the CCCS.[262]

As noted, these responsibilities are coordinated with key partners, notably CCCS and TBS (through the Chief Information Officer of Canada).

Summary

153. SSC was created in 2011 to provide information technology services to a group of federal organizations that represented the majority of the government's spending on digital infrastructure. Over time, the SSC mandate evolved, along with the range of security and defence services it provides to its partners and clients. From its establishment as an organization serving 43 core partners, SSC has grown to provide services to 160 different organizations across the Government of Canada. While SSC's secure-by-design approach has facilitated a robust security posture for organizations that receive its key cyber security and cyber defence services, the inconsistencies in service provision to mandatory and optional clients introduces challenges and cyber security risks to the rest of government. The Committee returns to this consideration in its assessment.

[262] TBS, Government of Canada Cyber Security Event Management Plan (CSEMP), 2019. Some of these responsibilities have shifted to CCCS with its creation in 2018.

The Communications Security Establishment

154. The Communications Security Establishment (CSE) is at the centre of the government's framework for cyber defence. It collects intelligence on threats to government systems and networks, operates a sophisticated, layered defensive network of sensors that identifies and blocks those threats, and provides direction and advice to government organizations (and increasingly, to Canadians and private sector organizations) to strengthen their own information technology security. This section discusses CSE's authority to conduct these activities and the governance mechanisms used to control those activities and to ensure CSE's accountability to the Minister of National Defence. It then describes the cyber defence activities themselves and the results they have achieved to date. The Committee uses case studies of actual cyber incidents to illustrate key issues.

CSE cyber-related mandates and authorities

155. On December 18, 2001, Parliament passed the *Anti-terrorism Act*.[263] That Act amended the *National Defence Act* to add Part V.1, Communications Security Establishment. For the first time, CSE's authority to conduct its activities was founded not in the Crown prerogative but in statute. The Act provided CSE with a threefold mandate:

(a) the acquisition and use of foreign intelligence in accordance with government intelligence priorities;
(b) the provision of advice, guidance and services to help protect electronic information and infrastructures of importance to the government; and
(c) the provision of technical and operational assistance to federal law enforcement and security agencies.

156. The Act contained significant control and accountability measures. Activities conducted under parts (a) and (b) of the mandate could not be directed at Canadians nor at any person in Canada, and CSE was obligated to implement measures to protect the privacy of Canadians in the use and retention of intercepted information. It also created a ministerial authorization regime to allow CSE to intercept private communications for the purposes of foreign intelligence collection and for protecting the computer systems of the Government of Canada.[264] This was a critical change: prior to these authorities, CSE's ability to fulfill its foreign intelligence collection and information protection mandates was in steady decline due to the emergence of an increasingly digital global information infrastructure. To conduct certain activities to protect government systems and networks, CSE obtained ministerial authorizations once certain

---

[263] *National Defence Act*, R.S.C., 1985, c. 95, s.s. 273.64(1) and 273.64(2), (prior to passage of Bill C-59 and the *Communications Security Establishment Act*), http://laws-lois.justice.gc.ca/eng/acts/n-5/20181218/P1TT3xt3.html.
[264] *National Defence Act* (s. 273.69) clarified that Part VI of the *Criminal Code* did not apply to the interception of a private communication when authorized by the Minister. The ministerial authorization regime also applied to CSE signals intelligence activities; these activities are not further discussed here.

conditions were met.[265] CSE's three-fold statutory mandate and these authorizations allowed CSE to develop and conduct novel cyber defence activities on government computer systems or networks, notably active network security testing activities to *measure* the security status of specific government systems and networks and cyber defence activities to *protect* specific government systems and networks.[266]

157. On June 21, 2019, the *Communications Security Establishment Act* (CSE Act) received Royal Assent. The CSE Act significantly changed CSE's mandate, authorities, immunities and oversight. The Act provided the organization with an overarching mandate as "the national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance."[267] The Act provided five aspects to the CSE mandate: foreign intelligence; cyber security and information assurance; defensive cyber operations; active cyber operations; and technical and operational assistance.[268] The aspects of CSE's mandate of most relevance to this review are cyber security and information assurance and defensive cyber operations.

Cyber security and information assurance

158. The CSE Act *sets* the CSE mandate in the area of cyber security and information assurance. That mandate is to provide advice, guidance and services to help protect federal institutions' electronic information and information infrastructures, and those of non-federal institutions designated as being of importance to the Government of Canada.[269] The Act also *enables* the cyber security and information assurance mandate by permitting CSE to acquire, use and analyze information from the global information infrastructure (e.g., Internet and mobile communications systems), namely through ministerial authorizations, or from other sources (e.g., publicly available information) to provide its advice, guidance and services.[270] In practice, this means that information acquired as part of CSE's foreign intelligence aspect can be used to support CSE's cyber security and information assurance aspect, including its acquisition and use of information from government networks and computers.

---

[265] These conditions were: the interception was necessary to identify, isolate or prevent harm to government systems; information could not be obtained through other means; the consent of persons whose information would be intercepted could not be obtained; only information that was necessary to identify, isolate or prevent harm to government systems would be used or retained; and that satisfactory measures were in place to protect the privacy of Canadians. *National Defence Act*, R.S.C., 1985, c. 95, s.s. 273.65(1) to 273.65(4). (Prior to passage of Bill C-59 and the *Communications Security Establishment Act*), http://laws-lois.justice.gc.ca/eng/acts/n-5/20181218/P1TT3xt3.html.

[266] *National Defence Act*, R.S.C., 1985, c. 95, s.s. 273.65(9), (prior to passage of Bill C-59 and the *Communications Security Establishment Act*). http://laws-lois.justice.gc.ca/eng/acts/n-5/20181218/P1TT3xt3.html. The Act explicitly limited the application of the ministerial authorization regime to "federal institutions" as defined in the *Official Languages Act*.

[267] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 15(1), and 15(2).

[268] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 15(1), and 15(2).

[269] References in this section will be made to the designation of non-federal institutions as being of importance to the government. Where the Committee uses "government" in these context, its reference is to the Government of Canada.

[270] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 17 (*a*)(i) and (*a*)(ii), and 17 (*b*).

159. A key component of this aspect are ministerial authorizations. Authorizations allow CSE, despite any other Act of Parliament, to access the information infrastructure of a federal institution or a non-federal institution designated as a system of importance to the government and to acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure, for the purpose of helping to protect it (in this context, from disruption, unauthorized use or mischief).[271] For non-federal institutions, CSE is permitted to access their systems for these purposes only if the institutions have first been designated under ministerial order as of importance to the Government of Canada, and when the owner or operator of that non-federal institution has requested CSE's assistance in writing.

Defensive cyber operations

160. Defensive cyber operations are distinct from activities conducted as part of the cyber security and information assurance mandate and inherently carry more risk because of their invasive and potentially disruptive nature. The CSE Act sets the defensive cyber operations aspect of the CSE mandate to carry out activities on or through the global information infrastructure to help protect federal institutions' electronic information and information infrastructures and electronic information and information infrastructures designated as being of importance to the Government of Canada.[272]

161. This means that CSE can conduct defensive cyber operations to defend a government network or the network of an entity designated by the Minister from cyber attack. Such operations can include:

- gaining access to a portion of the global information infrastructure;
- installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure;
- doing anything that is reasonably necessary to maintain the covert nature of the activity; and
- carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of those activities authorized by the authorization.[273]

162. Defensive cyber operations are conducted under ministerial authorization. These authorizations allow CSE, despite any other Act of Parliament or of any other foreign state, to carry out cyber operations on or through the global information infrastructure, and to conduct any activity specified in the authorization in the furtherance of the defensive cyber operations aspect of the CSE mandate.[274]

---

[271] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 27(1) and (2); and *Criminal Code* para. 184(2)(*e*).
[272] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 18(*a*) and (*b*).
[273] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 31(*a* to *d*).
[274] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 29(1).

Authorized activities, constraints, limitations and conditions

163. The CSE Act sets a number of constraints, limitations and conditions on the conduct of activities under the cyber security and information assurance and the defensive cyber operations aspects of CSE's mandate. First, the CSE Act prohibits the organization from directing its activities at any Canadian, no matter their location, or at any person in Canada, and stipulates that CSE activities must not infringe on these individuals' rights under the *Canadian Charter of Rights and Freedoms*.[275]

164. Second, for both the cyber security and information assurance activities and the defensive cyber operations, the CSE Act permits CSE to:

- acquire, use, analyze, retain or disclose publicly available information;
- acquire, use, analyze, retain or disclose infrastructure information for the purpose of research and development, for the purpose of testing systems or conducting cyber security and information assurance activities on the infrastructure from which the information was acquired – this allows for the collection of descriptive information on a network (e.g., pertaining to its configuration) to support the conduct of cyber security and information assurance activities; and
- test or evaluate products, software and systems, including testing or evaluating them for vulnerabilities.[276]

165. Third, where CSE is permitted to perform cyber security or information assurance activities on a network, it may identify or isolate malicious software, prevent that malicious software from harming the network, or otherwise mitigate any harm such malicious software may cause to the network. CSE may also analyze information to be able to provide advice on the integrity of supply chains and on the trustworthiness of telecommunications, equipment and services.[277]

166. Fourth, ministerial authorizations play an important role in authorizing CSE to conduct higher-risk activities in these areas. For example:

- ministerial authorization is required for any cyber security and information assurance activity that risks contravening an Act of Parliament, involves the acquisition of information from the information infrastructures of federal institutions or non-federal institutions designated as of importance to the government, that interferes with the

---

[275] *Communications Security Establishment Act*, S.C. 2019, c.13, s. 76, s.s. 22(1). The same prohibition exists for activities conducted under the foreign intelligence and active cyber operations aspects of the mandate. Regarding the technical and operational assistance aspect of its mandate (where CSE may provide technical or operational assistance to a federal law enforcement or security agency, the Canadian Forces or the Department of National Defence), CSE is subject to the same limitations imposed by law on that entity. This includes any restrictions imposed by an applicable warrant.

[276] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 23(1).

[277] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 23 (3)(*a*) and (*b*).

reasonable expectation of privacy of a Canadian or a person in Canada, or that risks infringing on the *Canadian Charter of Rights and Freedoms*;[278] and

- all activities conducted as part of a defensive cyber operation must be carried out under a valid ministerial authorization, and such authorizations may only be issued if the Minister has consulted the Minister of Foreign Affairs. In addition, the CSE Act prohibits defensive cyber operations from being directed at any portion of the global information infrastructure that is in Canada.[279]

While defensive cyber operations must always be conducted under ministerial authorization, other activities (e.g., the provision of advice or guidance to a government department) do not require authorization as they do not present the same risks to Charter rights or of contravening an Act of Parliament. The role ministerial authorizations play is discussed in greater detail in the next section on governance.

Governance of CSE cyber defence activities

167. The CSE Act is the foundation for CSE's authorities, accountabilities and governance. The Act provides four broad categories of governance instruments for CSE activities. The most relevant to cyber defence are ministerial authorizations, ministerial directives, ministerial orders, and CSE's internal operational policies and guidance. Each of these instruments is described below.

Ministerial authorizations

168. Ministerial authorizations have been a part of the governance architecture for CSE activities since 2001. Under the CSE Act, the Minister of National Defence may issue three authorizations of relevance to cyber defence:

- **Cyber security authorizations – federal infrastructures:** These permit CSE to access the network of a federal institution and to acquire and use any information on that network to protect it from mischief, unauthorized use or disruption. The Minister has issued two authorizations under the Act for the years 2019–2020 and 2020–2021.[280]
- **Cyber security authorizations – non-federal infrastructures:** These permit CSE to access the network of a non-governmental entity designated by the Minister as of importance to the government and to acquire and use any information on that network to protect it from mischief, unauthorized use or disruption. The Minister has issued one such authorization since the passage of the CSE Act.[281]

---

[278] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 22(4).
[279] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 22(2)(*a*) and (*b*), and 29(2).
[280] Mischief, unauthorized use or disruption are in reference to para. 184(2)(*e*) of the *Criminal Code*. The two authorizations are: CSE, "Cybersecurity Authorization for Activities on Federal Infrastructures," Ministerial authorization, August 1, 2019; and CSE, "Cybersecurity Authorization for Activities on Federal Infrastructures," June 30, 2020.
[281] CSE, "Cybersecurity Activities on Non-Federal Infrastructures," Ministerial authorization, November 7, 2019.

- **Defensive cyber operations authorizations:** These permit CSE to carry out any activity specified in the authorization on or through the global information infrastructure to help protect federal institutions' electronic information and information infrastructures, and electronic information and information infrastructures designated as of importance to the government. The Minister has issued two authorizations in this area for the years 2019–2020 and 2020–2021. In the case of the first authorization, no defensive cyber operations were conducted during its period of validity (this issue is described further below).[282]

169. The Minister may issue an authorization only for activities that the Minister believes are reasonable and proportionate and where satisfactory measures are in place to protect the privacy of Canadians. Consistent with new obligations in the CSE Act, the Chief of CSE must submit a written application to the Minister, which includes facts and descriptions that allow the Minister to conclude that there are reasonable grounds to believe that the requested authorization is necessary and that the conditions for issuing it are met.[283]

170. All ministerial authorizations, including those for cyber security and for defensive cyber operations, must include specific elements of information, notably:

- the activities or class of activities that CSE is being authorized to carry out and which of those activities would otherwise be contrary to any other Act of Parliament;
- the persons or class of persons who are authorized to carry out the activities identified in the authorization;
- the activities authorized must be reasonable and proportionate, having regard for the objective to be achieved, and the nature of the activity to be performed;
- any terms, conditions or restrictions that the Minister considers advisable in the public interest, or advisable to ensure the reasonableness and proportionality of any activity included in the authorization; and
- anything else reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activity authorized by the authorization.[284]

171. Five additional conditions must be met for the Minister to approve an authorization for cyber security (both for federal systems and systems designated as of importance):

- any information acquired will be retained for no longer than is reasonably necessary;
- for federal systems, the consent of all persons whose information may be acquired could not reasonably be obtained and, for non-federal systems, the owner or operator of the system must request the assistance in writing;

---

[282] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 18(*a*) and (*b*); 27(1) and 27(2); 29(1) and (2); and 34(1). The two authorizations are: CSE, "*** Defensive Cyber Operations," Defensive Cyber Operations Authorization, September 5, 2019; and CSE, "*** Defensive Cyber Operations," Defensive Cyber Operations Authorization, August 25, 2020.
[283] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 33(1).
[284] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 35(*a* to *i*).

- any information acquired is necessary to identify, isolate, prevent or mitigate harm to the electronic information or infrastructure in question;
- the measures CSE has in place to protect privacy will ensure that information acquired on Canadians or a person in Canada will be used, analyzed or retained only if it is essential to identify, isolate, prevent or mitigate harm to the electronic information or infrastructure in question; and
- any additional terms or conditions the Minister deems necessary to further protect the privacy of Canadians and of persons in Canada.

All ministerial authorizations for cyber security are reviewed by the Intelligence Commissioner to ensure that the conclusions leading to their granting are reasonable. Ministerial authorizations are not legally valid until the Intelligence Commissioner has approved them in writing.[285]

172. Two additional conditions must be met for the Minister to approve an authorization for defensive cyber operations:

- the objective of the authorization could not reasonably be achieved through other means;
- information will be acquired only in accordance with an existing authorization under the CSE Act for foreign intelligence, cyber security or an emergency authorization as stipulated in the Act.

Moreover, CSE must not "cause, intentionally or by criminal negligence, death or bodily harm to an individual" and CSE must not "willfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy."[286] Because defensive cyber operations may implicate Canada's relations with other countries, the Minister of National Defence may issue such an authorization only after consulting the Minister of Foreign Affairs.[287] The Intelligence Commissioner does not review authorizations for defensive cyber operations.

173. Ministerial authorizations are valid for up to one year and may be amended, subject to certain conditions.[288] The Minister may also provide an emergency authorization for up to five days for activities conducted as part of the cyber security and information assurance aspect of the CSE mandate, and must notify the Intelligence Commissioner of that authorization. Thereafter, CSE must apply to the Minister for an authorization consistent with normal procedures, including that the Intelligence Commissioner review and approve the application, if that authorization continues to be required.[289]

---

[285] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 28(1) and (2).
[286] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, paras. 32(1)(*a*) and (*b*). The Act also notes that "bodily harm" has the same meaning as in para. 2 of the *Criminal Code*, which describes "any hurt or injury to a person that interferes with the health or comfort of the person and that is more than merely transient or trifling in nature."
[287] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 29(2).
[288] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 36(1) to 36(4); 37(1) to 37(4); 38; and 39(1) and (2).
[289] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 40(1) to 40(4), 41 and 42.

Ministerial directives

174. CSE activities must be consistent with the Minister's direction, including in areas of cyber security and information assurance and defensive cyber operations. Prior to the CSE Act in 2019, CSE had received ministerial directives in the following areas:

- Government of Canada Intelligence Priorities;
- Accountability to the Minister;
- The Privacy of Canadians;
- The Collection and Use of Metadata;
- The Management of Third-Party Relationships; and,
- Avoiding Complicity in Mistreatment by Foreign Entities.

With the exception of the Ministerial Directive on the Government of Canada Intelligence Priorities, all of the ministerial directives issued under the *National Defence Act* ceased to be in effect when the *National Defence Act* provisions on CSE were repealed on August 1, 2019 and the CSE Act came into force. CSE's only active ministerial directive (on the Government of Canada Intelligence Priorities) was issued in 2019. That directive is based on the intelligence priorities approved by Cabinet and directs CSE's efforts to collect and share intelligence, and to collaborate with other parties. It requires CSE to report annually to the Minister on its efforts to support the priorities. Cyber and Cyber-Enabled Operations is one of four priorities in the directive.[290]

Ministerial orders

175. The Minister of National Defence may issue two types of ministerial orders to CSE in relation to cyber defence activities:

- orders to designate the devices, networks and information of non-federal institutions as of importance to the Government of Canada; and
- orders to designate entities with whom CSE is permitted to share information related to Canadians or persons in Canada or Canadian businesses when necessary to help protect the information or systems of federal institutions or critical infrastructures.[291]

Designating non-federal institutions as of importance to the government

176. The CSE Act stipulates that the Minister may issue a ministerial order to designate any electronic information or any information infrastructures as of importance to the Government of Canada. This means that where electronic information or information infrastructures exist outside of federal institutions (e.g., a research network or an aspect of critical infrastructure), the Minister may designate those entities as systems of importance to the Government of Canada, thereby permitting CSE to provide them services. Where those services risk contravening an

[290] CSE, Ministerial Directive to CSE on the Government of Canada Intelligence Priorities for 2019-2021, June 21, 2019; CSE, "NSICOP Cyber Defence Report- CSE Feedback on First Draft," pp.4, July 9, 2021.
[291] CSE, *Governance*, undated, https://cse-cst.gc.ca/en/accountability/governance.

Act of Parliament (e.g., the *Criminal Code*), or infringing the *Canadian Charter of Rights and Freedoms*, CSE must obtain a ministerial authorization to conduct cyber defence activities to defend these designated systems.[292]

177. The Minister of National Defence has issued two orders to designate classes of electronic information and information infrastructures as of importance to the government: the first in July 2019, then repealed and updated by a second order in August 2020. The order does not expire and includes:

- Canada's 10 critical infrastructure sectors: government (federal, provincial, territorial, municipal and Indigenous), energy and utilities, information and communications technology, finance, food, health, water, transportation, safety, and manufacturing;
- information related to the well-being of Canadians and the infrastructure lawfully containing it;
- entities that support the protection of electronic information and information infrastructures of importance to the government;
- multilateral organizations located in Canada in which the government is a member;
- registered Canadian federal, provincial, and territorial political parties and their electronic information and information infrastructures; and
- post-secondary educational institutions.[293]

178. The order does not *obligate* CSE to provide its advice, guidance or services to any entity in those designated areas. Rather, CSE must obtain a request from an entity for assistance and then consider a number of factors to determine if the entity falls within the classes designated by the Minister.[294] Should CSE determine that a non-federal institution is an entity within the classes designated by the Minister, it may then provide its advice, guidance and services to help protect that entity from cyber attack. Should CSE determine that the deployment of its cyber defence sensors or the conduct of a defensive cyber operation would be required to protect the entity (or sector), it must seek a ministerial authorization.[295] As of May 2021, CSE deployed cyber defence sensors under ministerial authorization to one non-federal institution identified as falling under the first ministerial order to defend the entity from an attack by *** a state actor (see case study 2).

---

[292] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 21(1).
[293] CSE, *Overview Note for the Minister of National Defence. Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada.* June 17, 2019; CSE, *Ministerial Order. Communications Security Establishment Canada. Electronic Information and Information Infrastructures of Importance to the Government of Canada*, July 22, 2019; and CSE, *Order. Communications Security Establishment. Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada,* August 25, 2020.
[294] These factors include whether the entity provides services on which the integrity of other sectors depends or the nature of the harm resulting from the disruption of services provided by the entity. A full list of factors is in CSE, Electronic Information and Information Infrastructures of Importance to the Government of Canada, CSE Ministerial Order, July 22, 2019.
[295] CSE, *Overview Note for the Minister of National Defence. Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada.* June 17, 2019.

Case study 2: Use of a new authority

[*** Three paragraphs were revised to remove injurious or privileged information. ***] In 2019, CSE detected efforts by a state to compromise the network of a Canadian company.[296] The state was well-known for its sophisticated attacks against western targets. CSE identified the company as an organization that provided services to a number of critical infrastructure clients and formally identified the company as a system of importance to the government, consistent with the Minister's ministerial order.

CSE blocked related state cyber activity on all government networks and determined that government departments were unaffected. CSE informed the company of the compromise and, in response to its request for assistance, worked with the company to stop the attack.

This case study represents the first use of a novel authority provided to CSE only months earlier. While the Committee is reluctant to draw significant conclusions, it notes two issues. First, this incident shows that authorities must be flexible enough to respond to new challenges. As CSE officials noted, this type of deployment was not what was envisioned when the statute was drafted; rather, the authority was meant to enable longer-term, more proactive collaboration with non-federal organizations, particularly telecommunications companies. Nonetheless, the authority allowed CSE to respond to a sophisticated attack on a company that provided valuable services to critical infrastructure, including the government itself.

Second, it underlines the importance of speed. It took time from when CSE detected anomalous cyber activities to when it helped the company take protective measures and obtained ministerial approval to assist. This is not a criticism: the fact that CSE identified the attack at all is a testament to how closely it monitors threats to Canada. But such attacks must be addressed "at the speed of cyber." An advanced threat actor can compromise a system, steal data or undermine system functionality in a worryingly short period. The government must continue to consider practical means for CSE to respond to rapidly emerging cyber threats while ensuring adequate ministerial control and accountability.

Designating recipients of identifiable information about Canadians or Canadian businesses

179. The CSE Act stipulates that the Minister may issue an order to designate persons and classes of persons to whom CSE may disclose information that could be used to identify a Canadian or a person in Canada. In the context of the cyber defence activities, it may do so if the disclosure is necessary to help protect the electronic information and information infrastructures of federal institutions, or non-federal institutions designated by the Minister as of importance to the government. In practice, this means that CSE may disclose information if it was acquired, used or analyzed as part of activities carried out under the cyber security and information assurance aspect of the CSE mandate, including private communications intercepted as part of such activities.[297]

---

[296] This case study is drawn from CSE, ***, NSICOP briefing, February 26, 2021; CSE, ***, 2019; CSE, *Application to the Minister of National Defence for Cybersecurity Activities on Non-Federal Infrastructure* ***, 2019; and CCCS, NSICOP appearance, February 26, 2021.

[297] *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76, s.s. 44(1) and (2), and 45.

180. The Minister of National Defence has issued two orders to designate classes of persons to receive information disclosed by CSE that relates to a Canadian or a person in Canada: the first in July 2019, then repealed and updated by a second order in August 2020. That order does not expire and designates several persons and classes of persons to whom disclosure is permissible if the disclosure of that information is necessary to help protect the electronic information and information infrastructures of federal institutions, or those of systems designated as of importance to the government. Entities covered by the order include:

- owners or administrators of a computer system or network used by the government or by any non-federal institution entity that has been designated to be of importance to the government;
- persons or classes of persons who operate under the authorities of federal institutions having a cyber defence coordination or mitigation mandate, where such persons have an operational requirement for the receipt of such information (e.g., SSC, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police);
- authorized persons or classes of persons within foreign entities with which CSE has established arrangements, including the Five Eyes partners, ***, and foreign computer security incident response teams; and
- foreign or domestic cyber security organizations that support the protection of electronic information and information infrastructures of importance to the government and entities involved in cyber security research and development with which CSE has a partnership.[298]

Internal operational policies

181. CSE's internal operational policies are known as its Mission Policy Suite. The Mission Policy Suite: Cybersecurity provides policy principles and requirements to guide personnel working under the cyber security and information assurance aspect of CSE's mandate to conduct their activities lawfully. All information acquired by CSE as part of the cyber security and information assurance aspect of its mandate is handled in accordance with the Mission Policy Suite.[299]

182. Specifically, the Mission Policy Suite: Cybersecurity governs the acquisition, use (analysis), retention and disclosure of information in the conduct of CSE's operations. The policy also addresses four critical areas in the conduct of cyber defence activities:

---

[298] CSE, "Disclosure of Information Related to Canadians and Persons in Canada (Cybersecurity and Information Assurance)," CSE Ministerial Order, July 22, 2019; CSE, *Order. Communications Security Establishment. Designating Recipients of Information Related to a Canadian or a Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspects of the CSE Mandate,* August 25, 2020.
[299] CSE. "Annex III: Relevant Policy Principles and Control Measures," *Application to the Minister of National Defence for Cybersecurity Authorization. Activities on Federal Infrastructures*. July 26, 2019; CSE, Mission Policy Suite: Cybersecurity, November 5, 2020; CSE, *End of Authorization Report for the Minister of National Defence. Cybersecurity Authorization for Activities on Federal Infrastructures. August 29, 2019 – July 30, 2020*, undated; and CSE, *Authorization Cybersecurity Activities on Non-Federal Infrastructures*, November 7, 2019.

- CSE (and the CCCS) authority to conduct activities under the cyber security and information assurance aspect of the CSE mandate;
- the core policy principles with which the CSE must comply when conducting activities under the cyber security and information assurance mandate – lawfulness, necessity and reasonableness, privacy protection, and transparency and accountability;
- the electronic information and information infrastructures of importance (otherwise known as systems of importance) to the government; and
- general accountability requirements for CCCS personnel operating under the cyber security mandate.[300]

183. The Mission Policy Suite: Cybersecurity details the specific policy areas, legal obligations, and operational processes and procedures that CSE personnel must follow in the conduct of cyber security and information assurance activities. The policy is meant to enhance privacy protection measures, manage operational risks, and enhance the reasonableness and proportionality of CSE activities. Based on the Mission Policy Suite, several control measures may be applied to CSE activities, including:

- **elevated approvals:** employed as a risk control measure, elevated approvals may be required for cyber defence activities that may implicate privacy, legal, operational, partnership or reputational risk for the Government of Canada; and
- **tagging and tracking of information:** information acquired or disclosed to CSE is tagged to indicate its origin, and its access, use and handling requirements. Once tagged, information is tracked throughout its life cycle to control its access, retention and disposition, limitations on use and sharing. This also help CSE to fulfill its obligations under ministerial authorization.

The Mission Policy Suite: Cybersecurity also establishes how long CSE may keep information; provides a guide for CSE's compliance teams to ensure that operational personnel have disposed of data in accordance with retention and disposition schedules; identifies when information about a Canadian must be suppressed; and provides dissemination controls and permissions for limiting access to particularly sensitive information (e.g., cyber defence or intelligence reports based on highly sensitive sources).[301] The Mission Policy Suite also requires CSE to obtain consent from a federal institution or a non-federal institution designated as of importance to the government prior to deploying its sensors to those institutions. All of the policy requirements identified in the Mission Policy Suite are incorporated into the ministerial authorizations provided to CSE.

---

[300] CSE, Mission Policy Suite: Cybersecurity, November 5, 2020; and CSE, "Annex III: Relevant Policy Principles and Control Measures," *Application to the Minister of National Defence for Cybersecurity Authorization. Activities on Federal Infrastructures*. July 26, 2019.

[301] CSE, Mission Policy Suite: Cybersecurity, November 5, 2020; and CSE, "Annex III: Relevant Policy Principles and Control Measures," *Application to the Minister of National Defence for Cybersecurity Authorization. Activities on Federal Infrastructures* (which was authorized), June 26, 2020.

CSE cyber defence activities

184. Under CSE, CCCS is the unified and authoritative source for cyber security in Canada. CCCS was created in 2018 by amalgamating three organizations: CSE's Information Technology Security branch, Public Safety Canada's Canadian Cyber Incident Response Centre and SSC's Security Operations Centre. CCCS is responsible to lead the government's response to cyber security events and to protect and defend Canada's cyber assets through targeted advice, guidance and direct assistance.[302] Within this broad mandate, CSE and CCCS conduct the following activities of direct relevance to cyber defence:

- provide advice and guidance to government departments and non-government partners;
- employ cyber defence sensors on government networks, including the monitoring, detection and response to cyber incidents;
- employ cyber defence sensors on non-government networks; and
- conduct defensive cyber operations.

The first two are by far the most common; the provision of cyber defence sensors to non-government networks and the conduct of defensive cyber operations stem from new authorities provided to CSE in 2019 and have yet to be widely employed. Each of these are described below.

Advice and guidance

185. CSE advice and guidance falls into three general categories. The first is authoritative direction. Under the Treasury Board Policy on Government Security, CSE is designated as the lead security agency and national authority for communications security. In that role, CSE issues information technology security directives to departments subject to the policy related to the implementation of standards and practices for the protection of classified information and data, and to secure or authenticate telecommunications information. CSE issued 11 such directives between 2012 and 2019.[303] These directives must be followed and implemented by subject government departments.

186. The second is alerts, advisories, and tailored information technology advice to organizations. Alerts and advisories are provided to government departments, critical infrastructure providers and the private sector. They cover a wide variety of topics, from vulnerability notifications related to critical infrastructure control systems, to web browser vulnerability warnings, to the sharing of unclassified intelligence community updates related to the targeting of government networks and critical infrastructure by state-sponsored advanced persistent threat actors. Receiving organizations may use the information to take practical

---

[302] CCCS, "About us," webpage, https://cyber.gc.ca/en/about-cyber-centre.
[303] CCCS, Directives, https://cyber.gc.ca/en/directives. The most recent directive is CCCS, *Mandatory Government of Canada Quantum Computing Threat Mitigation*, https://cyber.gc.ca/en/guidance/mandatory-gc-quantum-computing-threat-mitigation-itsb-127.

measures to defend their systems. Between December 2013 and May 2021, CSE issued 1,721 public alerts and advisories.[304]

187. The third category of advice and guidance is cyber defence reports and threat assessments. These documents vary in scope, topic and classification, and are written for a range of government audiences and the public to increase awareness of the cyber threat environment. These reports and assessments range from strategic assessments (the evolution of the cyber threat environment, the activities of specific states) to operational reports (overview of threats posed by specific cyber security events and vulnerabilities) meant to assist departments in defending their systems.[305]

CSE cyber defence sensors

188. CCCS has developed three types of cyber defence sensors. These are network-based sensors, host-based sensors and cloud-based sensors. Described in detail later, these sensors complement commercially available measures, such as anti-virus and firewall software, to fulfill two roles: to identify malicious cyber activity against government networks and non-federal institutions designated as of importance to the government, and to defend those networks from cyber attack.[306] Where deployed, CSE sensors form a layer of defences that constantly monitor computer systems and networks at various levels, block known threats, and identify anomalies. Information on anomalies is fed into sophisticated analytical systems to identify new, previously unknown malicious cyber behaviour. This information is then fed back into each sensor as new indicators of malicious cyber threat activity.[307]

189. CSE's cyber defence sensors use *** methods for the identification of malicious cyber threat activity, including [*** Two bullets were revised to remove injurious or privileged information. ***]:

- **Threat recognition:** When threats are recognized in the network or in data that CSE obtains through its sensors, an alert is generated. Based on the nature of the alert and the type of threat, a mitigation action may be triggered or CSE analysts may perform additional analysis to determine next steps.
- **Pattern detection:** CSE identifies patterns of behaviour that can indicate malicious cyber threat activity by noting instances of network, host or cloud activity that deviate from expected or normal behaviour. CSE can initiate defensive mitigations based on these patterns.[308]

---

[304] CCCS, "Alerts and Advisories," Webpage, https://cyber.gc.ca/en/alerts-advisories.
[305] CSE, Package 4: Table of Contents, September 22, 2020. This descriptive listing accompanying the provision of cyber threat reporting relates to threat assessments and vulnerability testing of Government of Canada systems, and mitigation measures applied in response.
[306] At the time of writing, all three sensor types had been deployed across numerous government departments and agencies. ***
[307] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.
[308] CSE, "CSE Cyber Defence Activities: For Approval," Memorandum for the Minister of National Defence, June 12, 2017.

190. Each sensor allows CSE to take mitigation actions to detect or counter a cyber threat. These mitigation actions can be done manually through interactive control by a CSE analyst or automatically through dynamic defence, that is, when verified, preset triggers respond to the presence of malicious cyber activity. Mitigation actions may include the blocking of a malicious connection at the network gateway or the removal of malware from a computer.[309] Information to identify new threats may also be reported to CSE partners and clients, inside and outside of government.

191. The deployment of defensive sensors involves two steps. The first is to obtain access to a network. Consistent with the authorities vested in individual organizations through the *Financial Administration Act*, CSE may only deploy its sensors with the informed consent of a network or system owner. In consenting to this access, the system owner provides CSE permission to access the network and electronic information stored therein.

192. The second step is to acquire information. CSE's sensors function by acquiring cyber threat information from the network or system in question. Because CSE cannot know in advance what data may be used maliciously, the breadth of information it acquires is extensive, including the content of traffic transiting a network (e.g., emails) and the metadata of those communications (i.e., information about a communication that can describe its creation, transmission and distribution). This information may contain private communications or information for which a Canadian or a person in Canada may have a reasonable expectation of privacy, and therefore requires a ministerial authorization (described above) to collect.[310]

193. Each of CSE's cyber defence sensors have gone through phases of technical development, proof-of-concept deployment at CSE and approval to deploy to government networks. Figure 2 outlines the timeline of cyber defence sensor development at CSE. The next section details each of the sensors. [*** A chart was revised to remove injurious or privileged information. ***]

---

[309] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.
[310] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.

- 2006: CSE develops the first network-based sensor
- 2010: CSE deploys first network-based sensor to government's Secure Channel Network
  - As a result, CSE discovers Chinese, state-sponsored compromise of Treasury Board Secretariat and Finance
- 2010: CSE develops first host-based sensor
- 2012: CSE deploys first host-based sensor sensors to the CSE network
- 2013: Development and proof-of-concept deployment at CSE of network-based dynamic defence capability
- 2014: first host-based sensor deployment outside of CSE, at the National Research Council
- 2014: first deployment of dynamic defence capability in response to HEARTBLEED
- 2015: CSE ***
- 2017: CSE begins a pilot project for host-based dynamic defence capability
  - June 2017: CSE uses host-based dynamic defence to remove malware from a computer at ***
- 2017: CSE develops first cloud-based sensor (a host-based sensor for cloud environments)
- 2019: Treasury Board mandates that government departments must have agreements in place with CSE to deploy cloud-based sensors in advance of initiating a cloud residency
- 2019: CSE ***
- 2019: CSE ***
- 2020: The Government of the United Kingdom announces it has improved its network defences through the adoption of Canada's (CSE's) host-based sensor technology, deploying at least 100,000 sensors

Figure 2: Cyber Defence Sensor Development Timeline[311]

Network-based sensors

194. The development of CSE's cyber defence sensors began in 2006 with *** network-based sensors. At the time, CSE operated sensors under ministerial authorization for several government departments to monitor the activity of a small number of foreign cyber threat actors, predominantly Russia and China.[312] In 2010, CSE deployed these *** sensors on the government's Secure Channel Network, which included dozens of different government organizations. Almost immediately, CSE discovered the compromise of TBS and Department of Finance networks by Chinese, state-sponsored cyber threat actors (see case study 1). In 2014, SSC approved the deployment of *** dynamic defences on its Secure Channel Network.[313] This allowed CSE to begin taking automated mitigation actions (dynamic defence) in response to significant attacks on government networks, including the 2014 Chinese attacks on the National Research Council and its portfolio partners and a widespread malware attack in 2014 (see case studies 3 and 4).

195. CSE's deployment of *** dynamic defences expanded as SSC replaced the Secure Channel Network with the Enterprise Internet Service as the government's main Internet

---

[311] CCCS, "Cyber Defence Activities," Deck and comments to NSICOP, October 2, 2020; CSE, "[Host-Based Sensor] (HBS) Deployment Priorities: Overview," Deck, January, 2020; CSE, "TOC – Response Package 11– CSE Response to RFI 2 – 6.B," Email to NSICOP Secretariat, January 15, 2021; and U.K. National Cyber Security Centre, "Introducing Host-Based Capability," Webpage, undated, https://www.ncsc.gov.uk/blog-post/introducing-host-based-capability-hbc.

[312] CSE began requesting ministerial authorizations in 2004 to conduct tailored network security testing and network monitoring for individual government departments. These requests followed compromises and attempted compromises by China (DND in 2003), and Russia (Foreign Affairs Canada in 2004). CSE, "Protection of DND Computer Systems and Networks: Request for Ministerial Authorization," Memorandum for the Minister of National Defence, January 19, 2004; and CSE, "Protection of Government of Canada Computer Systems and Networks. Foreign Affairs Canada: Request for Ministerial Authorization," Memorandum for the Minister of National Defence, June 16, 2005.

[313] CCCS, "Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck, October 2, 2020.

gateway. As of May 2021, *** federal institutions were active subscribers to SSC's Enterprise Internet Service and therefore protected by these sensors.[314] CSE also has separate bilateral arrangements to provide *** dynamic defences to a number of organizations.[315]

196. [*** This paragraph was revised to remove injurious or privileged information. ***] Dynamic defences are placed at entry points to a network (often referred to as a gateway, where a network connects to the Internet) to provide maximum visibility of digital traffic and information entering or exiting a government department. This allows CSE to identify threats targeting the information and networks of government departments and detect when systems have already been compromised. Not all threats are identified: malicious cyber actors may circumvent CSE's blocking. When known threats are identified, CSE's dynamic defences automatically block them at the network perimeter. As noted above, suspicious data is sent back to CSE, where it is subject to a sophisticated analytic process to identify suspicious or unusual (anomalous) behaviour.[316] When new threats are identified, CSE dynamic defences are directed to identify and block those threats thereafter. This dynamic defence of government networks is the key ingredient to successfully defending government networks, as information obtained at one department is applied to proactively defend other departments in an ongoing, continual process to strengthen government cyber defences.[317]

197. CSE sensors reinforce each other's unique capabilities. [*** Two sentences were revised to remove injurious or privileged information. The sentences noted that information acquired from one sensor is analyzed by CSE to detect malicious activity and the resulting indicators of compromise are distributed to other sensors, which in turn identify the same malicious activity and trigger mitigation responses for other organizations. ***].[318] The role of host-based sensors is discussed next.

---

[314] See paragraph 141.
[315] CSE, RFI-2 Item #3 – Provision of Cybersecurity Activities to Federal Institutions, December 23, 2020.
[316] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020; and CSE, "Cyber Defence Activities. A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck, October 2, 2020.
[317] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020; and CSE, "Cyber Defence Activities. A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck, October 2, 2020.
[318] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.

Case study 3: Dynamic defence and the HEARTBLEED vulnerability

[*** Five paragraphs were revised to remove injurious or privileged information. ***] On April 8, 2014, the United States publicly disclosed a vulnerability in open source encryption tools used to secure communications over computer networks and the Internet. The vulnerability, called HEARTBLEED, could be used to obtain confidential information, such as certificates securing and encrypting Internet communications, passwords and personal information.[319] CSE and SSC assessed the information and advised government network administrators to patch the vulnerability or disable their systems until they could.

On April 9, the Canada Revenue Agency (CRA) shut down two online tax services. On April 10, the Chief Information Officer of Canada issued government-wide direction to take vulnerable servers offline until patched. On April 11, SSC approved CSE's installation of dynamic defences on its Secure Channel Network. Within one month, these defences had blocked numerous instances of malicious HEARTBLEED traffic, protecting SSC and the government organizations that subscribed to the SSC secure Internet gateway. CSE also provided telecommunications service providers information to block HEARTBLEED attacks.

Treasury Board of Canada Secretariat described this incident as one of the most serious to affect the government. At the time, the government was poorly positioned to defend its networks from cyber attack. While CSE had deployed defensive tools to SSC, Global Affairs Canada, DND and CSE itself, it had not deployed dynamic defences and it was still in the early days of building its internal automation systems. As a result, multiple cyber threat actors used the vulnerability to extract information from government networks. In total, 12 government departments suffered remote exploitation and data exfiltration, including the theft of at least 900 taxpayer social insurance numbers from CRA.

After the attack, the government identified a number of challenges that remain of interest to the Committee today. These include the need for better governance of incident management, improving government-wide cyber security processes (for example, updated direction in areas such as vulnerability and patch management, privileged account access, and accurate and automated inventory of critical government systems), and strengthening the government's network perimeter.

Many of these problems have been addressed through new Treasury Board directives, more focused incident management protocols and the creation of SSC itself, which allows for quick and mandatory patching of vulnerabilities. As will be discussed later, however, challenges persist, notably that many departments still remain outside the secure perimeter and therefore unprotected by CSE's cyber defences. This leaves their information vulnerable to the most sophisticated actors and potentially creates pathways into government departments that are inside the perimeter. In addition, Treasury Board directives, SSC security configurations and CSE guidance are not universally followed, and in one case a lack of compliance caused preventable losses of data (see case study 6).

---

[319] This summary is based on TBS, HEARTBLEED: Government of Canada Lessons Learned and Management Response, September 2014; CSE, After Action Report HEARTBLEED, May 2014; CSE, Op HEARTBLEED: Timeline of events, September 2015; and CCCS, NSICOP appearances, November 27, 2020, and February 19, 2021.

Host-based sensors

198. CSE began the development of host-based sensors in 2010. At the time, CSE recognized that perimeter defences were only half the battle, and that an advanced cyber defence framework would require a tool that could identify the presence of advanced cyber threat activity on individual computers.[320] In 2012, CSE deployed the first host-based sensor on its own network as a proof of concept. In 2014, it deployed the first host-based sensor outside of CSE to the National Research Council and its science portfolio partners following the compromise of that agency's systems by China (see case study 4). By the end of 2014, CSE had deployed the sensor to 12 departments.[321] In 2015, it prioritized the rollout of host-based sensors to other government departments based on factors such as the likelihood that specific departments would be targeted by foreign states and where deployments would cover gaps in network-level monitoring.[322] By the end of 2020, CSE had deployed host-based sensors to *** departments, with a cumulative total of more than 500,000 host-based sensor deployments.[323] CSE has immediate plans to deploy this sensor to *** additional departments, and *** more federal institutions as part of ongoing efforts to expand host-based coverage of government departments. Current CSE planning on engagements with federal organizations would bring host-based sensor deployments to a total of *** organizations. The timeline to complete these roll-outs will vary from department to department, and will continue to prioritize organizations based on the sensitivity of the information they hold, their relative security posture and needs to cover ongoing gaps in monitoring.[324]

199. Host-based sensors are deployed on computers, workstations and servers, known as endpoint devices. These deployments allow CSE to acquire (or collect) information and to subsequently take mitigation actions to counter a cyber threat.[325] *** mitigation actions can be automated with host-based sensors, allowing for real-time, dynamic defence of individual computers. [*** Two sentences were deleted to remove injurious or privileged information. The sentences explained the installation of sensors. ***] Host-based sensors have the following functions:

---

[320] Scott Jones, Keynote speech, Countermeasure 2020, provided to NSICOP Secretariat, November 2020.
[321] See case study 4. See also CSE, HBS Deployment Priorities: Overview, Deck, January 2020. [*** The list of departments was deleted to remove injurious or privileged information. ***]
[322] CSE, "HBS Deployment Priorities: Overview," Deck, January 2020.
[323] CSE, "HBS Deployment Priorities: Overview," Deck, January 2020; CCCS, "Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck and comments to NSICOP, October 2, 2020; and Scott Jones, Remarks given to Countermeasure 2020, Keynote speech, Provided to NSICOP Secretariat November 2020.
[324] CSE, "HBS Deployment Priorities: Overview," Deck. January 2020; CCCS, "Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck and comments to NSICOP, October 2, 2020; CSE, TOC - Response Package 11 - CSE Response to RFI 2 - 6.B, January 15, 2021; CSE, HBS Deployment Priorities, October 22, 2020; and CSE, RFI-4 Item #5 – Follow-up questions on prioritization of HBS deployments, June 11, 2021.
[325] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.

- collecting information from a host, which is sent via an encrypted Internet link to CSE;
- analyzing and processing collected information to detect suspicious or anomalous activity occurring on a host machine;
- reporting anomalies, compromises and vulnerabilities to affected departments – with that information, CSE can provide mitigation recommendations (e.g., for patching or updating machines with new software, password resets or the removal of a machine from a network);
- removing malware from a host, either manually by a CSE analyst or automatically ***
- *** blocking or neutralizing malware; and
- ***

200. [*** This paragraph was revised to remove injurious or privileged information. ***] Host-based sensors collect several types of information. Similar to network-based sensors, this information may relate to a Canadian or to a person in Canada for which there is a reasonable expectation of privacy. As a result, host-based sensors are operated under ministerial authorization.[326]

[326] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020.

Case study 4: The need for enhanced endpoint protection

[*** Four paragraphs were revised to remove injurious or privileged information. ***] On June 18, 2014, CSE discovered a compromise of the National Research Council (NRC) by a Chinese state-sponsored actor.[327] The Chinese actor was believed to have been active since ***, and sought information related to foreign relations and trade, science and telecommunications technologies, energy and natural resources, and environment and climate change issues.

CSE determined that China had gained access to the NRC network by sending spear-phishing emails to NRC email accounts, and used its access to steal more than 40,000 files. The theft included intellectual property and advanced research and proprietary business information from NRC's partners. China also leveraged its access to the NRC network to infiltrate a number of government organizations.

At the time of the attack, the NRC network was not part of the SSC-managed Secure Channel Network and neither SSC nor CSE could use their sensors to observe China's activity on the NRC network. To see what was happening, CSE deployed host-based sensors for the first time outside of CSE. At the same time, CSE updated the dynamic defences it had just deployed on the Secure Channel Network (in April, in response to the HEARTBLEED attacks) to block China's attacks on other government departments. SSC also blocked NRC's connectivity to federal organizations.

The government's response to this incident was manual, extensive, costly, months-long and grew to include multiple departments. NRC informed its clients that their data may have been at risk. The costs of mitigating this attack was estimated at over $100 million and involved a years-long effort by the NRC, SSC and CSE to rebuild the NRC network with appropriate security safeguards built in from the start.

The incident exposed a number of challenges regarding the government's ability to protect its networks from cyber attack. Most notably, it highlighted the need to better protect the government's network perimeter, reduce and consolidate the number of Internet access points in use by government departments, and provide enhanced endpoint protection (through host-based sensors) outside of CSE. It also reinforced lessons learned in HEARTBLEED regarding the need for better governance of incident management and improvements to government-wide cyber security processes (e.g., patching of vulnerable applications and better control of privileged account access).

[327] This case study is based on: CSE, *** Presentation and supporting remarks to NSICOP, February 19, 2021; and TBS, *NRC Incident: Government of Canada Lessons Learned Report*, July 2015.

Case study 5: An attack against the Department of National Defence

[*** Three paragraphs were revised to remove injurious or privileged information. ***] In 2017, CSE discovered that a state sponsored actor had compromised a network of the Department of National Defence (DND). The actor stole significant amounts of data and used its presence to infect other networks. DND isolated the network, CSE updated its dynamic defences to protect other departments, and both cooperated with SSC to remove the actor's presence.[328]

This case study highlights important issues. The network contained several unpatched and unsupported applications and legacy operating systems, all of which were vectors of entry for the actor. Moreover, the network was not connected to SSC's Enterprise Internet Service and therefore not protected by CSE's defences. The network was, however, connected to a number of other government departments, introducing a risk of compromise to the broader government architecture had the actor been able to jump to those organizations' networks. On the other hand, CSE was able to deploy its defences and take immediate remedial action because of an existing ministerial authorization for cyber defence activities that already included DND.[329] In short, this case study underlines the dangers of maintaining unpatched, legacy systems with separate connectivity to the Internet outside of SSC's Enterprise Internet Service, and the importance of the existence of appropriate authorities to deploy necessary cyber defences.

[328] CSE, "Executive Summary," ***, 2017; and CSE, ***, 2018. See also DND, ***, 2017; DND, ***, 2017; DND, ***, 2018; DND, ***, 2018; and DND, ***, undated.
[329] CSE, "Cyber Defence Activities," 2017–2018 CSE ministerial authorization, June 22, 2017.

Cloud-based sensors

201. As discussed earlier, the government is increasingly using cloud environments as part of its modernization plans for information technology systems and infrastructure. In 2017, TBS issued the Direction on the Secure Use of Commercial Cloud Services, obligating subject departments to comply with prescriptive security guardrails before receiving approval for initiating a cloud tenancy. In 2019, TBS obligated departments to include cloud-based sensors as part of their cloud implementation, and CSE and SSC started onboarding departments for cloud-based sensor deployments.[330] The deployment of cloud-based sensors was further accelerated as a result of the COVID-19 pandemic. In May 2020, TBS established service-specific guardrails for Microsoft Office 365 and SSC fast-tracked, in collaboration with TBS and CSE, the migration of departments to cloud-based email and collaboration services to respond to significant demands for remote work. CSE and SSC collaborated to rapidly add cloud-based sensors to *** organizations. As a result, CSE is now positioned to provide monitoring services for all departments who transition their email services to SSC-brokered cloud services.[331]

202. Cloud-based sensor deployments are meant to protect the tenancy of federal institutions in cloud environments, and to augment protection services offered by network-based and host-based sensors.[332] [*** Five sentences were deleted to remove injurious or privileged information. The sentences described CSE operations. ***]

- ***
- ***
- ***

As with network-based and host-based sensors, cloud-based sensors may collect information for which a Canadian or a person in Canada may have a reasonable expectation of privacy. As a result, deployments of cloud-based sensors are operated under a ministerial authorization.

---

[330] TBS, Remarks during appearance with NSICOP, November 27, 2020; CSE, *TOC - Response Package 11-CSE Response to RFI 2 - 6.B*, January 15, 2021. See also paragraphs 115–118 describing the TBS Cloud Adoption Strategy and security requirements of the TBS Direction on the Secure Use of Commercial Cloud Services; and the Government of Canada Cloud Guardrails at https://github.com/canada-ca/cloud-guardrails.

[331] CSE, TOC - Response Package 11-CSE Response to RFI 2 - 6.B, January 15, 2021.

[332] CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization (which was authorized), June 26, 2020; and CSE, "Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)," Deck, October 2, 2020.

Case study 6: A state attack against a Crown corporation and government systems

[*** Five paragraphs were revised to remove injurious or privileged information. ***] In 2020, CSE discovered that a state had compromised the network of a Crown corporation. The state used its presence on the corporation's network to compromise several government departments and scan multiple others for vulnerabilities. It likely attacked other Crown corporations. CSE and SSC blocked links between the corporation and the rest of government, and determined that the state had accessed significant amounts of information. The attack was mitigated. Later, CSE discovered that the state had compromised a government department and attempted to compromise others. These attacks were also mitigated.[333]

This case study highlights two issues. First, cyber defence sensors are effective, but they cannot work if they are not deployed. The Crown corporation is not subject to Treasury Board direction, did not use SSC's Enterprise Internet Service, and has yet to implement CSE's recommendation to adopt it. Second, even where a department is subject to Treasury Board and SSC direction, it can refuse it: three months prior to the state compromise, SSC shut down a department's weak single-factor authentication service only to have its decision reversed by departmental officials, despite a stronger alternative being available within two weeks. This was a key factor in the cyber attack.

[333] This summary is based on: CSE, ***, 2020; CSE, ***, 2021; CSE, ***, 2020; SSC, ***, 2020; and CSE, NSICOP appearance, ***, 2020.

Defensive cyber operations

203. Defensive cyber operations are one of the newest aspects of CSE's five-part mandate. The operations are meant to protect the electronic information and infrastructures of federal organizations and non-federal organizations designated as systems of importance to the government. Thus far, CSE has received two year-long ministerial authorizations to conduct such operations, ***.[334] In neither case were operations actually conducted; in the first year, normal cyber defence activities successfully mitigated the threat and obviated the need for a separate operation and in the second year, planned operations had not proceeded to the operational stage.[335] As a result, the Committee limits itself to providing an explanation of these operations and may return to the issue in the future.[336]

204. Defensive cyber operations require ministerial authorization. Without this authorization, defensive cyber operations would risk contravening one or more acts of Parliament (e.g., the *Criminal Code*). This can include activities that involve fraudulent behaviour, falsification of materials or information, manipulation of computer hardware or software without the permission of the system owner, and interacting with threat actors at the time that actor commits an offence. Operations may be used in three circumstances:

- when a cyber threat is of such sophistication that neither commercially available defences nor CSE's classified sensors are sufficient to counter it;
- when a compromise has progressed to a stage that already-deployed sensors are no longer capable of mitigating it; and
- when a cyber threat is of such scope and scale, affecting so many federal institutions and designated non-federal entities, that deploying sensors could not be done in a timely manner to mitigate the threat.[337]

205. The CSE Act requires that defensive cyber operations be conducted on portions of the global information infrastructure outside of Canada, must not be directed at Canadians or any person in Canada and must not infringe the Charter. These operations would involve *** to install, maintain, copy, distribute, search, modify, disrupt, delete or intercept anything, or interact with anyone, in order to achieve objectives of protecting government networks and those of entities designated as of importance to the Government of Canada. In practice, this means that CSE may:

---

[334] *** CSE, "*** Defensive Cyber Operations," Defensive Cyber Operations CSE Authorization, August 25, 2020.
[335] [Two sentences were deleted to remove injurious or privileged information. They described CSE operations. ***] CSE, "*** Defensive Cyber Operations. September 6, 2019 – August 25, 2020," End of Defensive Cyber Operations authorization report for the Minister of National Defence, undated; and CSE, "DCO MA Information Package for NSICOP," Email to NSICOP Secretariat, June 14, 2021.
[336] This summary is based on CSE, "*** Defensive Cyber Operations: (For Approval)," Application by the Chief, CSE, to the Minister of National Defence for an authorization under subsection 29(1) of the CSE Act, September 4, 2019; and CSE, briefing to NSICOP Secretariat, May 28, 2021.
[337] CSE, "*** Defensive Cyber Operations: (For Approval)," Application by the Chief, CSE, to the Minister of National Defence for an authorization under subsection 29(1) of the CSE Act, September 4, 2019.

- ***
- ***
- ***
- ***
- ***

206. [*** This paragraph was revised to remove injurious or privileged information. The paragraph described CSE techniques. ***] Under the current ministerial authorizations, defensive cyber operations are conducted to achieve certain objectives, but are not meant to be used to collect information.

- ***
- ***
- ***
- ***

Results and outcomes

207. CSE measures the success and value of its cyber defence program by tracking the degree to which its sensor program is able to isolate and prevent harm to federal electronic information and information infrastructures or non-federal institutions designated as of importance to the government. This data is provided annually to the Minister of National Defence in applications for ministerial authorizations and subsequent reporting. These metrics are provided in Table 2.

Year	2015–2016	2016–2017	2017–2018	2018–2019	2019–2020
Host-based sensors deployed (departments)	161,012 (***)	313,781 (***)	345,160 (***)	404,891 (***)	583,809 (***)
Network-based sensors deployed (departments) [338]	Consistent data was not available during this period.[339]				*** (***)
Cloud-based sensors deployed (departments)	N/A	N/A	N/A	*** (***)	*** (***)
Malicious traffic blocked (daily)	282 million	474 million	693 million	1.6 billion	1.3 billion
Compromises (advanced persistent threats)	*** (***)	*** (***)	*** (***)	*** (***)	*** (***)
Compromises with exfiltration of data	***	***	***	***	***
Cyber defence reports	961	1,110	2,070	1,193	4,379

[338] [*** Two sentences were deleted to remove injurious or privileged information. They described the number of departments protected by CSE cyber defences. ***]

[339] [*** Two sentences were deleted to remove injurious or privileged information. They described the number of departments protected by CSE cyber defences. ***]

Sources: Data drawn from CSE, "Ministerial Authorization Year End Report: 2015–2016", Undated; CSE, Ministerial Authorization Year End Report: 2018–2019. Undated; CSE, "Interim Ministerial Authorization Year End Report: May 2019 – October 2019," Undated; CSE, "End of Authorization Report for the Minister of National Defence – Cybersecurity Authorization for Activities on Federal Infrastructures: August 29, 2019–July 30, 2020," Undated; CSE, HBS Deployment Priorities, October 22, 2020; CSE, "CSE Cyber Defence Activities," Memorandum for the Minister of National Defence, June 12, 2017; CSE, CSE, "Cyber Defence Activities," Memorandum for the Minister of National Defence, May 30, 2016; CSE, "CSE Cyber Defence Activities," Memorandum for the Minister of National Defence, June 11, 2018; and CSE, "Activities on Federal Infrastructures," Application to the Minister of National Defence for Cybersecurity Authorization, July 26, 2019.

Table 2: Cyber Defence Sensors; Measuring Outcomes

208. CSE's cyber defence sensors cover a significant portion of government networks. As of November 10, 2020, CSE provides some or all of its cyber defence sensors to a total of *** federal institutions, either through those organizations subscribing to the SSC Enterprise Internet Service or various bilateral agreements including with a handful of agencies or Crown corporations not subject to Treasury Board directives.[340] As a result, Canadian government networks enjoy the most advanced cyber security measures of "any national government in the world."[341]

209. Nonetheless, many government organizations do not benefit from these protective measures deployed by CSE, as they are not obligated to do so. The total inventory of federal government organizations is 169. These include everything from commonly known departments (e.g., Global Affairs Canada), to agencies like the Canadian Security Intelligence Service or CSE, service-oriented entities (e.g., the Canada Border Services Agency), Crown corporations (e.g., Export Development Canada), and separate agencies (such as the offices of the Information Commissioner and Privacy Commissioner of Canada). Some of the organizations, including the Secretariat to this Committee, obtain their information technology services through an organization that SSC and CCCS protects. Others do not, obtaining their information technology and Internet connectivity through private sector companies. The reasons for this vary and include concerns about independence from government and cost of service, but it leaves those organizations worryingly vulnerable to the loss of their own data and to inadvertently acting as a hidden vector into the government's protected systems through electronic links maintained with related federal departments, thereby also putting the government's data at risk. The Committee discusses this issue in its assessment.

210. As part of its reporting to the Minister of National Defence, CSE tracks the number of times it has used, retained or disclosed private communications or solicitor-client communications incidentally collected under its cyber security ministerial authorizations. How CSE counts this number has changed drastically in the last several years. Far from being a

[340] [*** One sentence was deleted to remove injurious or privileged information. It listed the Crown corporations protected by CCCS. ***]. CSE, RFI-2 Item #3 – Provision of Cybersecurity Activities to Federal Institutions, December 23, 2020.

[341] CSE, "Cybersecurity Authorization for Activities on Federal Infrastructures. August 29, 2019 – July 30, 2020," End of Authorization Report for the Minister of National Defence, undated.

simple issue of methodology, those changes reveal important things about the risks posed to Canadians' reasonable expectation of privacy by CCCS cyber defence activities.

211. Prior to 2018, CSE automatically tracked and recorded any email collection with at least one end in Canada as a private communication. This resulted in CSE reporting to the Minister on the retention of hundreds of thousands of communications.[342] In March 2015, the CSE Commissioner completed a combined review of CSE's cyber defence activities conducted under ministerial authorizations issued between 2009 and 2012 and found that the vast majority of private communications unintentionally intercepted by CSE contained only malicious code and efforts to tailor a message to entice the target to open its content. The Commissioner concluded that those intercepted private communications contained no consequential information or exchange of any personal information and therefore should not be considered "private communications" as defined by the *Criminal Code*.[343]

212. [*** One sentence was deleted to remove injurious or privileged information.***] CSE revised the interpretation of what constitutes a private communication under cyber security ministerial authorizations: CSE now reports fewer than 100 such interceptions a year.[344] In the CSE Commissioner's view, the previous practice distorted the privacy risk implications of CSE's cyber defence activities, while the new methodology "should provide a more accurate and meaningful measure of the privacy implications resulting from CSE activities."[345] The fact that CSE cyber defence activities entail relatively few privacy risks to Canadians or owners of systems and networks on which CSE sensors are deployed should be an important factor for organizations that cite independence as the reason for remaining outside of the government's cyber defence framework, an issue to which the Committee returns in its assessment.

Summary

213. The Communications Security Establishment (CSE) is at the centre of the government's framework for cyber defence. It collects intelligence on threats to government systems and networks, operates a sophisticated, layered defensive network of sensors that identifies and blocks those threats, and provides direction and advice to government organizations (and increasingly, to Canadians and private sector organizations) to strengthen their own information technology security. CSE's cyber defence capabilities have evolved to counter cyber threats of increasing sophistication, and as they have been deployed to increasing numbers of federal organizations, have grown to play an ever-increasing role in the government's ability to defend

---

[342] CSE, "Ministerial Authorization Year End Report: 2018–2019," undated.
[343] CSE Commissioner, *Subject: Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization*, March 29, 2019.
[344] For clarity, CSE notes that a recognized private communication is one that contains, "substantive content … that is sent without malicious intent, but may contain malicious content. For example, an email sent by a non-malicious originator that, unbeknownst to the originator, contained a malicious component such as a malicious link or embedded malicious code, may still contain recognized substantive content with a reasonable expectation of privacy." CSE, "Ministerial Authorization Year End Report: 2018–2019," undated.
[345] CSE Commissioner, Subject: Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization, March 29, 2019.

its networks from cyber attack. This section discussed CSE's authority to conduct cyber defence activities, described the development and use of each of CSE's cyber defence sensors, and the internal governance mechanisms used to control those activities and to ensure CSE's accountability to the Minister of National Defence. The next section of the report describes the governance mechanisms in place to manage the conduct of cyber defence activities across government.

Part IV: Governance of Cyber Defence

214. Cyber defence is a team sport. The government has several interdepartmental governance mechanisms to support proper administration, effective program operations and accountability of cyber defence. When a cyber attack occurs, the government uses specific committees to coordinate a response commensurate with the attack's severity and scope. This section explains the role that various committees play in developing strategic cyber defence policy, supporting the effective management of information technology security initiatives affecting government-wide operations, and responding to cyber security incidents. It then describes the Cyber Security Event Management Plan, the government's primary mechanism to establish departmental roles and responsibilities for cyber security incident response. This description includes how the government sets its response levels for cyber attacks, the roles of various governance bodies and the phases of the process.

Strategic considerations

215. The Deputy Ministers' Committee on Cyber Security (DM Cyber Security) is the primary body responsible for cyber security coordination, policy and strategic cyber objectives. Co-chaired by Public Safety Canada and the Communications Security Establishment (CSE), its mandate is to develop and lead Canada's cyber security policies and operations in support of the government's economic and social priorities. The purpose of DM Cyber Security is to:

- identify policy, legislative and program opportunities to ensure that Canada's 21st-century digital economy is secure by design, and that Canada is recognized internationally for leadership on cyber security issues; and
- oversee the evolution and progress of the implementation of Canada's National Cyber Security Strategy.[346]

DM Cyber Security's core membership consists of deputy ministers from 14 organizations, including those with operational or policy responsibilities for cyber security (CSE, Treasury Board of Canada Secretariat – TBS, and Public Safety Canada), lead security agencies (Privy Council Office, the Canadian Security Intelligence Service – CSIS, Department of National Defence and Canadian Armed Forces – DND/CAF, the Royal Canadian Mounted Police – RCMP), critical infrastructure sectors (Health Canada, Natural Resources Canada, Transport Canada) and deputies from economic departments that exercise authority within Canada's critical infrastructure sectors (Department of Finance; Innovation, Science and Economic Development Canada).

216. DM Cyber Security replaced a previous committee (see paragraph 86 in the section on the evolution of cyber defence 2010 to 2018) and differs from its predecessor in important ways.

---

[346] Canada, Deputy Ministers' Committee on Cyber Security Terms of Reference, 2019.

First, the revised mandate of DM Cyber Security is to enhance collaboration between security departments, economic departments and critical infrastructure in the recognition that issues of cyber security touch a range of departmental responsibilities. Second, leadership for this committee was expanded from the previous Deputy Minister of Public Safety to include the Chief of the Communications Security Establishment (CSE) as co-chair, reflecting the creation of CCCS and its central role within cyber defence.[347] The new DM Cyber Security held its first two meetings in June and September 2020 to discuss collaboration between security departments, economic departments and critical infrastructure; cyber operations and threats; and the National Cyber Security Strategy. The Committee has since met every 8 weeks.

217. DM Cyber Security is supported by an Assistant Deputy Ministers' Cyber Security Committee (ADM Cyber Security). As a supporting committee, ADM Cyber Security's mandate mirrors that of the DM committee: to develop and lead Canada's cyber security policies and operations in support of the government's wider economic and social priorities. It coordinates these issues among departments and prepares issues for DM consideration and decision. The purpose of ADM Cyber Security is to:

- guide policy direction and operations for issues related to cyber security;
- develop cyber security-related priorities for member departments and agencies;
- monitor progress on the implementation of Canada's National Cyber Security Strategy;
- consider emerging cyber issues and threats; and
- review and prepare items for DM Cyber Security.

ADM Cyber Security is co-chaired by the Senior ADM, National Security and Cyber Security Branch of Public Safety Canada, and the Deputy Chief of CSE. Its core membership mirrors that of DM Cyber Security. It is supported by the Director General Committee on Cyber Security and its operational sub-group, the Director General Cyber Operations Committee.[348] ADM Cyber Security meets every 10 weeks, or on an ad-hoc basis as needed.[349]

218. The Deputy Minister Committee on Enterprise Priorities and Planning (DM Enterprise Priorities and Planning) is another governance body with responsibilities related to strategic, enterprise-wide cyber security considerations. As stated in the Policy on Service and Digital, DM Enterprise Priorities and Planning serves as a senior-level body responsible for improving the government's client service and government operations through the strategic management of enterprise services, information, data, information technology and cyber security.[350] While the previously discussed DM Cyber Security focuses on enhancing cooperation across the security and intelligence community and with economic departments and critical infrastructure, DM

---

[347] Canada, Deputy Ministers' Committee on Cyber Security Terms of Reference, 2019.
[348] Public Safety Canada, Assistant Deputy Ministers' Committee on Cyber Security, 2019; and Public Safety Canada, DG Cyber Operations Committee Terms of Reference, November 16, 2018.
[349] Public Safety Canada, Assistant Deputy Ministers' Committee on Cyber Security Record of Discussion, August 13, 2020.
[350] TBS, Policy on Service and Digital, s. 4.1.1.1.

Enterprise Priorities and Planning focuses primarily on the management of information technology and service delivery.

219. After the Treasury Board Policy on Service and Digital was approved, DM Enterprise Priorities and Planning created new terms of reference to better reflect the importance of discussing horizontal issues, with a focus on improving the delivery of services to Canadians.[351] Consistent with the Policy on Service and Digital, the purpose of DM Enterprise Priorities and Planning as it pertains to cyber security is to:

- establish priorities for information technology shared services and assets, and information technology investments and procurements that are government-wide or require the support of Shared Services Canada (SSC);
- support and enable departments to adopt enterprise solutions for common services;
- review and endorse the SSC investment and work plan, and provide input to SSC transformation initiatives;
- provide strategic advice and recommendations on matters relating to the management and delivery of government services to individuals and businesses; and
- endorse enterprise architecture and government-wide standards for information technology.

220. DM Enterprise Priorities and Planning is co-chaired by the Secretary of the Treasury Board and the Chief Operating Officer of Service Canada. Its membership consists of eight senior government executives, including the Chief of CSE, the President of SSC, the Chief Information Officer of Canada and the Deputy Clerk of the Privy Council.[352]

Operations, policy and programs

221. The Assistant Deputy Minister Information Technology Security Tripartite Committee (ADM Tripartite) is the primary body responsible for the governance of interdepartmental information technology security initiatives. It is chaired by the TBS Chief Technology Officer of Canada and its membership is made up of assistant deputy ministers from CSE, SSC, TBS and invited departments. It provides direction and oversight to its supporting Director General Information Technology Security Tripartite (DG Tripartite).

222. The ADM Tripartite has a two-part mandate. First, it serves as a decision-making body supporting the effective design, delivery and management of priority information technology security initiatives affecting internal government systems and government-wide operations. Under this part of its mandate, ADM Tripartite is responsible for:

---

[351] TBS, Deputy Minister Committee on Enterprise Priorities and Planning Speaking Notes, August 22, 2019.
[352] TBS, Deputy Minister Committee on Enterprise Priorities and Planning Terms of Reference, undated.

- providing advice to set strategic and policy direction in the area of information technology security for the government;
- providing direction and guidance to the DG Tripartite (further described below) to ensure that information technology security strategic priorities are aligned with the enterprise direction established by the ADM Tripartite; and
- raising key initiatives and recommendations to senior-level executive committees for consideration or decision.

The second part of the ADM Tripartite mandate is to manage major cyber events, discussed further below. This committee meets on an ad hoc basis and has held four meetings since 2016.

223. The DG Tripartite plays an active role in supporting the ADM Tripartite. Its mandate is to:

- align information technology security strategic priorities with the enterprise direction established by the ADM Tripartite or ADM Enterprise Priorities and Planning;
- provide advice, guidance, oversight and direction to CSE, TBS and SSC to address significant issues and obstacles that may affect progress of enterprise information technology security initiatives;
- monitor the progress and health of select CSE, TBS and SSC horizontal projects and initiatives related to enterprise information technology security; and
- provide the ADM Tripartite with strategic cyber security guidance and reporting on the status, risks and issues related to CSE, TBS and SSC enterprise information technology security initiatives.

The DG Tripartite is chaired by TBS and its membership comprises officials from TBS, CCCS, SSC and invited guests. It meets about 10 times a year. On July 9, 2021, NSICOP was informed that in March 2021, the ADM Tripartite and three other ADM-level governance committees were amalgamated to create the new ADM Quad Committee. The DG Tripartite supports this new committee.[353]

Incident response

224. The Cyber Security Event Management Plan is the primary mechanism to govern departments' roles and responsibilities in the context of cyber security incident response. It provides an operational framework for the management of cyber security events that affect or threaten to affect the government's ability to deliver programs and services to Canadians. Pursuant to the Policy on Government Security, TBS first issued the plan in 2015 and updated it in 2019. TBS is currently reviewing the plan to ensure that the roles and responsibilities of the newly created CCCS are clearly articulated.[354] The Cyber Security Event Management Plan

---

[353] TBS, Director General IT Security Tripartite Committee Terms of Reference, February 2021; TBS, Assistant Deputy Minister Quad Draft Terms of Reference, March 3, 2021; and TBS, "NSICOP Review - TBS Comments on Draft Final Report (9-July-2021)," pp.6, July 9, 2021.
[354] CCCS, NSICOP appearance, October 30, 2020.

applies to all departments and agencies subject to the Policy on Government Security (currently 110 departments and agencies).[355]

Cyber Security Event Management Plan response levels

225. The plan establishes four levels that govern the government's response to cyber security events targeting its systems and networks. Response levels are based on two factors: severity and scope. The severity of a cyber incident is measured through standardized departmental assessments of injury, including harm to the health and safety of individuals; financial losses or economic hardship to an individual, business or the economy; effects on government programs and services; effects on civil order or national sovereignty; damage to the reputations of individuals, businesses or the government; and damage to federal-provincial relationships and international relations. The scope of the event is measured by the number of people, organizations, facilities, systems and geographic areas affected by the event and the expected duration of the injury. Based on their analysis, departments identify to CCCS the expected results of a compromise. These range from low harm (e.g., physical harm or financial stress to an individual, minor impediment to departmental service delivery) to very high (e.g., major damage to public safety, national security or the economy, loss of confidence in government).

226. Based on this departmental input, CCCS and TBS use a standardized matrix to calculate the government's overall response level.[356] The matrix considers whether a compromise is likely to affect one or more internal government programs or services, whether external services are affected, and whether there is potential for broader propagation of the injury. Based on these values, CCCS and TBS determine the response level required, ranging from Level 1 (requires the least government coordination) to Level 4 (requires the most government coordination). There are four government response levels:

- **Level 1:** The severity and scope of the cyber security event does not engage the plan. Such events require only a departmental response and the standard level of government coordination. Departments respond consistent with standard internal procedures, apply regular preventive measures, and communicate with CCCS for advice and guidance.
- **Level 2:** The severity and scope of the cyber security event surpasses a Level 1 event and engages the plan: a limited government-wide response is required. All primary stakeholders are on heightened alert for cyber activity. This includes monitoring departmental and government-wide sensors (e.g., network- and host-based sensors) to verify whether the event has affected other departments and ensuring that any real or potential impact is contained and mitigated. Specialized stakeholders are engaged when a threat or incident is related to crime, terrorism or national defence.
- **Level 3:** The severity and scope of the cyber security event surpasses a Level 2 event and requires an immediate and comprehensive government-wide response. Event

[355] The Treasury Board Policy on Government Security is applicable to those organizations listed in schedules I, I.1 (Column I), II, IV, and V of the FAA.
[356] TBS, Government of Canada Cyber Security Event Management Plan (CSEMP), 2019.

response at this level is coordinated through the plan's governance structure, with departments and agencies given ongoing direction on how to proceed.

- **Level 4:** These events represent the highest level of severity and scope and are considered "severe catastrophic events" that affect multiple government institutions, confidence in government or other aspects of the national interest. They require the invocation of Public Safety Canada's Federal Emergency Response Plan, which identifies the mechanisms and processes to facilitate a harmonized federal government response to emergencies.[357] There have been no Level 4 cyber events or incidents to date.[358]

Cyber security events are dynamic and their injury and scope may increase or decrease as the event unfolds. As a result, the government may escalate or de-escalate its response level over the course of a particular cyber security event. Decisions regarding the escalation and de-escalation of the government's response level are made by increasingly senior governance bodies, described below.

Cyber Security Event Management Plan governance bodies

227. Three categories of stakeholders are involved in the Cyber Security Event Management Plan. TBS and CCCS are primary stakeholders and are engaged in all Level 2 and 3 events. CCCS would also provide advice and guidance in the context of a Level 1 event. Public Safety Canada, SSC, the RCMP, CSIS and DND/CAF are specialized stakeholders and are engaged for confirmed cyber security incidents or threat events based on their specific mandates and areas of expertise. The plan lists other stakeholders who play different roles in cyber defence, including the Chief Information Officer of Canada, the Government Operations Centre, the Privy Council Office, the CSE Canadian Committee on National Security Systems (responsible for the governance and protection of Top Secret systems),[359] the Director General Event Response Committee, and external partners, such as private sector suppliers and other levels of government.

228. The plan establishes three governance bodies that are responsible for prioritizing the government's response to serious cyber incidents and managing the escalation of responses to a cyber security event:

- **Event Coordination Team:** This group of working-level stakeholders is co-chaired by TBS and CCCS. It is activated for Level 2 events or when invoked by other governance bodies for Level 3 or 4 events. The Event Coordination Team works with stakeholders to recommend courses of action and to ensure the Executive Management Team (below) is apprised of events.

---

[357] Public Safety Canada, Federal Emergency Response Plan, 2011, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-eng.pdf.
[358] CSE, Briefing to NSICOP Secretariat, March 11, 2021.
[359] CSE, Canadian Committee on National Security Systems, Bulletin, Edition 1, March 2018.

- **Executive Management Team:** This Director General-level committee is co-chaired by TBS and CCCS. It is triggered for Level 3 events. The Executive Management Team provides the Event Coordination Team with strategic direction and ensures that senior government officials are apprised of events.
- **ADM Tripartite:** This assistant deputy minister-level committee is chaired by the TBS Chief Technology Officer. It is triggered for Level 3 events. This committee provides direction to the Executive Management Team to respond to and mitigate an event. It is also responsible for ensuring that deputy ministers are apprised of events. During Level 4 incidents, the ADM Tripartite would support the Federal Emergency Response Plan Committee of assistant deputy ministers as appropriate. CCCS's Deputy Chief and SSC's ADM, Networks, Security and Digital Services co-chair this committee.

For all three governance bodies, other government departments can be engaged as required. For example, when an event involves national security concerns or is believed to be criminal in nature, any of the governance teams may include officials from CSIS and the RCMP, respectively. Departments directly affected by specific threats or incidents are invited to participate in governance discussions.

Phases of the cyber security event management process

229. The cyber security event management process has four phases: preparation; detection and assessment; mitigation and recovery; and post-event activity.

230. Preparation involves ongoing steps to ensure that the government is ready to respond to cyber events. This includes establishing roles and responsibilities, documenting and testing plans and procedures, training personnel, and applying protective and preventive measures at the host, application and network levels of government information systems. As part of this ongoing phase, all of the Cyber Security Event Management Plan's stakeholders, including all departments and agencies to which the plan applies, are responsible for implementing such measures within their respective areas of responsibility. For its part, TBS is responsible for developing and maintaining the plan, coordinating regular exercises with all implicated stakeholders, and reviewing lessons-learned reports from past events to drive policy changes. CCCS is responsible for ensuring that departments and agencies are provided with the required advice and guidance to mitigate cyber threats and vulnerabilities in order to prevent cyber security incidents.

231. The second phase, detection and assessment, involves monitoring for emerging cyber security events and the assessment of their potential or actual impact on government service delivery, government operations or confidence in the government. As part of this phase, CCCS is responsible for monitoring technical sources and information reported by other stakeholders; the government's perimeter and all endpoints visible to CCCS; cloud-based environments; government networks and intelligence sources; and information from domestic and international sources. DND/CAF is responsible for monitoring all DND-managed networks. The RCMP and

CSIS are responsible for monitoring information from criminal surveillance sources and intelligence sources, respectively.

232. The Cyber Security Event Management Plan imposes a number of general and specific responsibilities. Generally, the plan obligates organizations to implement security controls consistent with the Policy on Government Security. It also obligates them to notify relevant authorities when an event falls under the domains of national security or law enforcement. More specifically, the plan obligates primary and specialized stakeholders to report detected cyber security events to TBS and CCCS and, when cyber events related to crime, terrorism or the military are detected, to the RCMP, CSIS and DND, respectively. When information is received indicating that a potential or actual cyber security event may exist, CCCS establishes the initial government response level in consultation with TBS, and other partners as necessary.

233. The third phase of the plan is mitigation and recovery. The purpose of this phase is to mitigate events before they become incidents and to contain and minimize the effects of incidents that have occurred to ensure the timely restoration of normal operations. Responses here may include installing patches, containment and mitigation of an incident, the invocation of business continuity and disaster recovery plans, or the temporary shutdown of vulnerable services.

234. The plan establishes the roles and responsibilities of applicable departments related to mitigation and recovery. For Level 3 events (and when determined by involved stakeholders, for certain Level 2 events), TBS provides strategic coordination, including strategic direction to departments on minimizing the government-wide effect of cyber events. The Government Operations Centre assumes this role for Level 4 events. For all events, CCCS provides operational coordination, including technical direction and advice to departments on mitigation or containment measures. All of the plan's primary and specialized stakeholders provide advice and guidance based on information received from their respective sources. Finally, departments and agencies must implement direction provided by CCCS and TBS within established timelines.

235. For all Level 3 and 4 incidents (and when determined by involved stakeholders, for certain Level 2 incidents), CCCS leads the development and implementation of a government-wide containment plan, and facilitates a targeted response. It also leads forensic examination and analysis of information technology systems in collaboration with affected departments. Affected departments and agencies and applicable service providers implement the containment plan, and SSC works to identify and report on affected or vulnerable systems.

236. The fourth phase of the Cyber Security Event Management Plan is post-event activity. In this phase, departments conduct post-event analysis and identify lessons learned to drive improvements to the cyber security event management process. As part of this phase, affected departments and agencies must produce a lessons-learned report and action plan, and contribute to government-wide post-event activities as required. CCCS collates departmental findings and produces a post-event report, including a timeline of events and root cause

analysis. For Level 3 events (and when determined by involved stakeholders, for certain Level 2 events), TBS must produce a lessons-learned report and action plan on behalf of the government and monitor implementation of the recommendations. The Government Operations Centre is responsible for producing a similar lessons-learned report and action plan for Level 4 events. Finally, all other stakeholders must support the development of government-wide lessons-learned reports and implement action items under their particular areas of responsibility.[360]

[360] TBS, Government of Canada Cyber Security Event Management Plan (CSEMP), 2019.

Part V: The Committee's Assessment of the Cyber Defence Framework

237. The Government of Canada has created the foundation for a strong and resilient cyber-defence framework. Where other states have recently fallen victim to successful cyber exploitations and ransomware attacks, Canada has either blocked the attacks or limited their worst effects. This was not always the case. Less than a decade ago, Canada sustained multiple, damaging cyber attacks against some of its core government institutions. The government's understanding of the nature of the threat was limited; its cyber defences ranged from poor at some departments to good at others; and governance suffered from little central coordination and siloed accountabilities. The Communications Security Establishment, Canada's foremost technical expert on cyber defence, was only just deploying its defensive sensors outside of a handful of government organizations and had yet to build the type of dynamic, automated defences necessary to fight the unrelenting attacks by cyber threat actors that mark the modern cyber threat environment.

238. By 2020, however, Canada had become a world leader in defending its networks from cyber attack. What changed is a lesson in three things: the importance of maximizing authorities in the face of change, responding to crises to not only solve the problem but also build for the future, and ensuring that authorities and organizations are fit for purpose. This does not mean that Canada is perfect: the government must continue to adapt in the face of changing threats and the evolution of technology, and the Committee makes a number of recommendations to do so. The Committee provides its assessment of these changes below.

The evolution of cyber defence in Canada: A virtuous cycle, but incomplete

239. The Communications Security Establishment (CSE) is central to this story. When it was provided statutory authority in 2001, CSE's activities to protect data and information technology systems were focused on system testing and high-end cryptology. The idea of cyber defence hardly existed. For several years thereafter, CSE was the only federal organization with the lawful authority to operate systems which risked intercepting private communications, such as firewalls and intrusion detection, that could protect a government network. Building on the organization's knowledge of signals intelligence, CSE developed and deployed proprietary defensive sensors to organizations being attacked by sophisticated state adversaries: China and Russia. These activities would have been impossible were it not for the government's willingness to allow CSE to use its novel authorities, that is, ministerial authorizations, in unexpected ways. Between 2002 and 2007, CSE experimented with new approaches and techniques while working to protect several departments from cyber attack. Its efforts were not without problems: in 2006, CSE was forced to pause its cyber defence activities for more than a year because those activities did not comply with legal obligations stemming from those authorities. After restructuring of the ministerial authorization program and its policy framework,

CSE resumed its cyber defence activities and deepened its expertise to detect and then block the most sophisticated cyber threats. Nonetheless, CSE's success in identifying threats and working with specific departments to implement mitigating measures likely would have continued to be constrained by the government's department-by-department approach to cyber defence.

240. [*** This paragraph was revised to remove injurious or privileged information. ***] Major cyber attacks proved to be important turning points. In 2010, CSE deployed its cyber defences onto the government's Secure Channel Network, where 75 departments had migrated their Internet access onto a single network managed by Public Works and Government Services Canada. That deployment revealed that China had penetrated the digital systems of a number of government organizations, key among them the Treasury Board of Canada Secretariat (TBS) and the Department of Finance, and stolen significant data. As a result, TBS directed all government departments to join the Secure Channel Network, which caused a number of departments to migrate their Internet access and laid the foundation for the evolution toward the Enterprise Internet Service several years later. In 2014, government networks were hit by the HEARTBLEED attack and the National Research Council suffered a separate, critical compromise involving the extensive theft of research information and scientific data. Both incidents were seminal events for the government, revealing broad system vulnerabilities and weaknesses in the government's cyber defence framework. They also resulted in CSE's first deployments of specific cyber defences. These deployments laid the groundwork for the further expansion and modernization of these services. These attacks also revealed significant problems in interdepartmental coordination and governance of major cyber incidents. As a result, TBS modernized various policies and directions to clarify roles and responsibilities and key departments took on increasingly prominent leadership roles in cyber incident response.

241. The government's development of new authorities and organizations was critical. In 2011, the government established a new organization, Shared Services Canada (SSC), to standardize and consolidate the purchase and provision of information technology and services across departments. Initially, the government emphasized the cost-saving elements of SSC's creation, but when the scope of the challenge was recognized (for example, SSC inherited a wide mix of new and outdated infrastructure), the government invested significant amounts to modernize the government's information technology infrastructure. Among other things, this meant that SSC would build security into the government's future technology modernization initiatives. From a cyber defence perspective, the most important changes arising from the creation of SSC were the increasing consolidation of government departments under the Enterprise Internet Service (more on this below) and the 'forcing function' played by SSC to oblige subject departments to patch their devices, systems and networks.

242. Important changes to the machinery of government continued in 2018 with the creation of a unit in CSE: the Canadian Centre for Cyber Security (CCCS). The amalgamation of three organizations, CCCS is the unified and authoritative source for cyber security in Canada. It is responsible for protecting and defending Canada's cyber assets through advice, guidance and direct operational assistance and, in collaboration with TBS, leading the government's response

to cyber security events. It continually modifies its approach to cyber defence, updating its network-based sensors to better detect and block malicious cyber behaviour, creating new host-based sensors to deepen the layers of network defence to the level of individual devices, and working to identify new threats through the accumulation and analysis of new intelligence and anomalous data. The promulgation of the *Communications Security Establishment Act* in 2019 may contribute further to these efforts by clarifying CSE authorities and immunities, including the addition of defensive cyber operations as a still-nascent tool to protect government systems in specific circumstances.

243. Over time, these changes have created a virtuous cycle. As more departments migrate to the SSC Enterprise Internet Service, the more they benefit from the sophistication of CCCS's dynamic defences. The more departments subscribe to CCCS cyber defence services for endpoint devices and cloud environments, the more the government's systems and data are secured from advanced cyber threats and cyber crime. The more data that CCCS obtains and analyzes from its expanding number of cyber defence sensors, the greater its ability to identify and block new cyber threats. Finally, the greater clarity over roles and responsibilities, governance, and incident response resulting from the creation of new departments and the promulgation of new authorities, policies and directives, the more the government can react quickly and deliberately to evolving threats. This should be true for the foreseeable future, as well. For example, TBS has mandated cloud-based sensor usage as part of the government's cloud security guardrails, thereby ensuring that strong security measures are built in by design. These changes and their ongoing evolution have produced clear results: Canada now sees increasingly fewer successful incidents of network penetration, data loss or damage.

Who is protected depends on who you ask

244. Perfection of this system is impossible: threats evolve, mistakes occur, defences fail. But improvement is always possible, and there are three important challenges to address. The first challenge is the inconsistent application of Treasury Board policies and directives. These instruments determine the scope of services afforded to government departments. The *Financial Administration Act* groups most federal organizations into specific schedules according to their mandate, governance structure and degree of independence, and provides the legal authority for Treasury Board to issue policies and directives. This facilitates the standardization of accountability requirements for organizations across government. However, the three primary Treasury Board instruments for cyber defence do not have the same scope of application. On the one hand, the Policy on Government Security and its related security directives, such as for the secure use of commercial cloud services, apply to 110 federal organizations; whereas the Policy on Service and Digital (and its derivative policies) and the Digital Operations Strategic Plan apply to 87 federal organizations. More broadly, these core elements of the government's administrative framework for cyber defence do not apply evenly (or in some cases, at all) to all of the Government of Canada's 169 organizations.

245. The second challenge is the way SSC's mandate and responsibilities for cyber security services are set out. A series of orders in council reference specific schedules of the *Financial Administration Act* to identify the departments to which SSC *must* provide its email, data centre, networking and endpoint device services, and those to which SSC *may* provide such services. The group of departments and agencies (SSC's core partners) to which SSC must provide services are the best-protected, as they receive the full complement of SSC services. For the group to which SSC may provide services (SSC's mandatory and optional clients), SSC's provision of services is essentially à la carte, where SSC provides some or all of its services on a cost-recovery basis. When government organizations find the costs for these services prohibitively expensive, they do not subscribe to them, leaving their data potentially vulnerable to exploitation. Yet these organizations have electronic links to other organizations' digital infrastructure, and may inadvertently provide access to a malicious cyber actor and potentially threaten the wider security of the government.

246. [*** This paragraph was revised to remove injurious or privileged information. ***] The third challenge is establishing a basis for expanding the number of government organizations receiving the protection of CSE's cyber defence program. CSE's mandate under the *Communications Security Establishment Act* provides the most expansive authority to provide cyber defence protection to federal institutions. Yet no government departments are obligated to use one or more of CSE's cyber defence sensors. While CSE currently provides one or more of its cyber defence sensors to *** percent of the 169 federal organizations that make up the Government of Canada, that leaves *** percent of federal organizations unprotected by any of CSE's cyber defence sensors. This causes problems. For one, it limits how much malicious cyber threat activity targeting government departments that CSE can observe. For another, it handicaps CSE's ability to react quickly when one or more unprotected departments are compromised in a cyber attack. Further, those organizations outside the umbrella of CSE's cyber defence sensors are themselves unlikely to know when they have been victimized. The one possible avenue of protection for these organizations would be where CSE's signals intelligence program, through its tracking of global cyber threats, obtains some indication of compromise and shares this information with CCCS. As discussed in case study 6 on the attack against a Crown corporation, such assistance would almost always come after data had been stolen and the integrity of the organization's system compromised. Going forward, maximizing the number of departments using all three types of sensors (where applicable) to protect their networks and information will be important to further protect the sensitive information held by government organizations and to ensure the provision of government services critical to Canadians.

The success and the gap: Securing Internet access in government

247. The question of which federal organizations use the government's secure Internet access underlies all three challenges. The creation of SSC's Enterprise Internet Service and its progressive adoption by departments have played a foundational role in strengthening the government's cyber defence framework. Further, the integration of CSE's *** dynamic defences

into the Enterprise Internet Service's Internet access points is arguably the single-most important defensive measure currently in the government's defensive framework. Extending this framework to all Government of Canada organizations requires addressing the three challenges described above.

248. First, departments should be applying Treasury Board policies and directives consistently. Since 2006, on four separate occasions, Treasury Board has issued 'mandatory' direction to government departments requiring them to use secure Internet services, most recently in 2018 as part of the Digital Operations Strategic Plan. This suggests that government organizations still exercise considerable discretion on which Treasury Board direction they accept and when. As of August 2021, 94 of 169 organizations subscribe to the Enterprise Internet Service. This includes nearly all organizations subject to Treasury Board policies, allowing the Committee to conclude that Treasury Board directives in this area have, eventually, been successful. Currently, the gap in the government's cyber defence framework is found among the 75 federal organizations *not* subject to Treasury Board direction in this area (more on this at paragraph 251 below). These organizations remain outside of the government's secure perimeter and the protection of CSE's cyber defences.

249. Second, the series of orders in council that establish SSC's mandate and responsibilities for cyber security services creates a patchwork of coverage for government organizations. The 94 organizations that receive or subscribe to the Enterprise Internet Service include 43 core partners, 27 mandatory clients and 24 optional SSC clients. For SSC's core partners, full SSC service provision includes the Enterprise Internet Service, and SSC is obligated to provide it. The mandatory and optional SSC clients that receive the Enterprise Internet Service have chosen to do so. In sum, these organizations contribute to and benefit from the framework's virtuous cycle, discussed above. In contrast, other federal organizations remain outside of the government's secure perimeter and the protection of CSE's cyber defences. Notwithstanding the vulnerability of these organizations, there is currently no plan or dedicated funding to incorporate some of them – namely, small departments and agencies – into SSC's wider security services, including in the Enterprise Internet Service. This is of significant importance. As the Committee heard:

> Internet gateways and the connections to the Internet were consolidated, starting with only the 43 large departments and agencies that fell under SSC's mandate. All small departments and agencies were left to their own devices. … Bringing them into the capabilities of SSC and CSE is imperative to being able to secure them. They need those services more than anyone.[361]

250. Third and finally, of the government organizations receiving the protection of CSE's cyber defence sensors, most are protected because they receive SSC's Enterprise Internet Service. Simply put, it is *the* means of acquiring this advanced protection from CSE. Of the *** federal organizations that receive one or more cyber defence sensors from CSE, *** of them benefit

[361] TBS officials, NSICOP appearance, November 27, 2020.

from *** dynamic defences. *** A few departments have their own bilateral agreements with CSE for deploying network-based sensors. The Committee lauds the efforts of SSC and CSE to enable such comprehensive protection for government systems. The concern now must be for establishing CSE cyber protection for those organizations that are not considered federal departments or agencies but are nonetheless digitally tied to the federal government.

Crown corporations and government interests

251. The 75 organizations that fall outside of Treasury Board direction and the Enterprise Internet Service are primarily Crown corporations and some government "interests." These corporations and interests have been created by the government for a variety of reasons and their mandates are meant to be independent of government direction to varying degrees. Most have considerable latitude to develop and secure their own information technology infrastructure, and many contract private sector companies to provide their infrastructure, host their data and protect their systems. Nonetheless, those organizations ultimately hold fiduciary and accountability requirements to the Crown. Most importantly for the purposes of this review, those organizations receive, hold and use the sensitive information of Canadians and Canadian businesses, information that is at risk of compromise by the most sophisticated of cyber actors, including states. Nonetheless, they are not required to adhere to Treasury Board policies meant to ensure the security of their information technology infrastructure. They are also excluded from the obligatory portions of SSC's enabling orders in council and therefore most do not obtain cyber defence services from SSC. The result is that most do not benefit from CSE's protection of the Enterprise Internet Service. This leaves those organizations worryingly vulnerable to the loss of their own data and, where they maintain electronic links with related federal departments, to inadvertently act as a vector into the government's protected systems, putting the government's data and systems at risk.

252. The Committee recognizes the importance of independence for Crown corporations and, where applicable, government interests. Independence of mandate is essential to protect the integrity of important areas of public policy, including the administration of justice or Canada's financial and economic systems. The Committee emphasizes two issues, however, in assessing whether independence of mandate should equate to exclusive control of data, systems and networks. First, it is clear that commercially available products and services are insufficient protection against the most sophisticated cyber threats. China and Russia have shown repeatedly that they are capable of penetrating well-defended systems and networks, particularly those that are not protected by equally advanced, state-supported cyber defences. The protection offered by CSE and SSC may be imperfect, but their combined cyber defences offer the greatest likelihood of protecting government data and the integrity of its systems in the future.

253. [*** This paragraph was revised to remove injurious or privileged information. ***] Second, Crown corporations and other government interests are targets of state cyber activities and cyber criminals, as demonstrated in specific incidents over the past several years. More generally, Russia, China and other states target critical infrastructure providers, including as

noted in the Committee's 2020 Annual Report, American natural gas and electricity providers. In Canada, some critical infrastructure organizations are federal Crown corporations. Based on the known behaviour of the most sophisticated state cyber threats, it would be naive to believe that those organizations would not be targets (or are not *currently* targets), either for the purposes of espionage or system degradation at some point in the future.

254. In the context of such organizations falling under the SSC and CSE protective umbrella, the Committee recognizes that organizations may have privacy concerns about CSE, in particular, monitoring system network traffic, email or web browsing. In that respect, the Committee takes note of the conclusions of the CSE Commissioner, who found that there were very low levels of privacy implications associated with CSE cyber defence activities conducted under ministerial authorization, an important consideration for organizations that cite privacy as a reason for remaining outside of the government's cyber defence framework. More importantly for the Committee, however, is the choice faced by Crown corporations and relevant interests: rely on the government, through a rigorous statutory mechanism with strong privacy safeguards and external review, to protect data, systems and networks from exploitation and potential degradation, or accept the relatively high probability that sophisticated cyber actors will compromise these organizations' systems in the future and steal the data they hold. For the Committee, the consequences of those choices are clear: not obtaining the government's cyber defence services means choosing to leave data and the integrity of systems vulnerable to the world's most sophisticated cyber threats.

Conclusion

255. The government is heavily dependent on its electronic infrastructure. It is how the government conducts its business and provides services to people in Canada. As a result, government systems and networks hold significant amounts of data of interest to foreign states, many of whom use sophisticated methods to try to infiltrate these systems and steal the data. Some of those states also increasingly target the very integrity of those systems themselves, leaving behind malware that could be triggered in the future to compromise the systems or render them inoperable. This is a threat to Canada's national security and the privacy of Canadians.

256. Over the last decade, Canada has built a strong cyber defence system to counter this threat. At its core are three organizations – Treasury Board of Canada Secretariat, Shared Services Canada and the Communications Security Establishment – that work closely together and with other government departments to build security into the government's cyber infrastructure and to strengthen its cyber defences. In its purest form, the system can be distilled into a few key elements:

- government systems fall within a single perimeter;
- the perimeter has a handful of access points to the Internet;
- those access points are monitored by sophisticated sensors that are capable of detecting and blocking known threats;
- defences are layered, with specialized sensors capable of detecting and blocking threats deployed on individual devices and to cloud environments;
- anomalies in network traffic are analyzed for new threats, information that is used to continually update *** cyber defences for threat identification and blocking; and
- departments continually update and patch their devices and systems under the coordinated direction, advice and guidance of the three organizations.

257. The current cyber defence system has not yet achieved this ideal. An overarching challenge is that the system is increasingly managed horizontally, while its foundational authorities remain vertical. This creates significant discrepancies: Treasury Board policies intended to secure government systems are not uniformly applied; individual departments and agencies retain considerable latitude whether to opt into the framework or to accept specific defensive technologies; and a large number of organizations, notably Crown corporations and potentially some government interests, neither adhere to Treasury Board policies nor use the cyber defence framework.

258. The threat posed by these gaps is clear. The data of organizations not protected by the government cyber defence framework is at significant risk. Moreover, unprotected organizations potentially act as a weak link in the government's defences by maintaining electronic connectivity to organizations within the cyber defence framework, creating risks for the

government as a whole. These challenges are well-known to the government. The Committee expects that its review and recommendations will help to address them.

Findings

259. The Committee makes the following findings:

F1. Cyber threats to government systems and networks are a significant risk to national security and the continuity of government operations. Nation-states are the most sophisticated threat actors, but any actor with malicious intent and sophisticated capabilities puts the government's data and the integrity of its electronic infrastructure at risk. (Paragraphs 25 - 67)

F2. The government has implemented a robust, 'horizontal' framework to defend the government from cyber attack. The Treasury Board of Canada Secretariat, Shared Services Canada and the Communications Security Establishment play fundamental roles in that framework. Nonetheless, this horizontal framework appears to be increasingly incompatible with the existing department-by-department 'vertical' authorities under the *Financial Administration Act*. (Paragraphs 95 - 213)

F3. The government has established clear governance mechanisms to support the development of strategic cyber defence policy, the effective management of information technology security initiatives affecting government-wide operations, and the government response to cyber incidents. This framework has evolved over time in response to changes in government policies, machinery and the cyber threat environment. (Paragraphs 214 - 236)

F4. The strength of this framework is weakened by the inconsistent application of security-related responsibilities and the inconsistent use of cyber defence services. These weaknesses include:

- Treasury Board policies relevant to cyber defence are not applied equally to departments and agencies. As a result, not all organizations must fulfill the same responsibilities, requirements and practices. This creates gaps in protecting government networks from cyber attack. (Paragraphs 95 - 125)
- Crown corporations and potentially some government Interests are known targets of state actors, but are not subject to Treasury Board cyber-related directives or policies and are not obligated to obtain cyber defence services from the government. This puts the integrity of their data and systems and potentially those of the government at significant risk. (Paragraphs 251 - 254)
- Cyber defence services are provided inconsistently. While Shared Services Canada provides some services to 160 out of 169 federal organizations, only 43 of those receive the full complement of its services. The Communications Security Establishment provides services in support of Shared Services Canada and through agreements with some individual organizations. This inconsistency introduces risks to those organizations and to the rest of government and limits the overall efficacy of CSE's cyber defence program. (Paragraphs 126 - 153)

Recommendations

260. The Committee makes the following recommendations:

R1. The government continue to strengthen its framework for defending government networks from cyber attack by ensuring that its authorities and programs for cyber defence are modernized as technology and other relevant factors evolve, including to align them with the horizontal framework for cyber defence that has emerged over the last decade.

R2. To the greatest extent possible, the government:

- Apply Treasury Board policies relevant to cyber defence equally to departments and agencies;
- Extend Treasury Board policies relevant to cyber defence to all federal organizations, including small organizations, Crown corporations and other federal organizations not currently subject to Treasury Board policies and directives related to cyber defence;
- Extend advanced cyber defence services, notably the Enterprise Internet Service of Shared Services Canada and the cyber defence sensors of the Communications Security Establishment, to all federal organizations.

Government response to recommendations

Recommendation (R1) The government continue to strengthen its framework for defending government networks from cyber attack ensuring that its authorities and programs for cyber defence are modernized as technology and other relevant factors evolve, including to align them with the horizontal framework for cyber defence that has emerged over the last decade.
Response Agreed. Public Safety, Communications Security Establishment, and Treasury Board of Canada Secretariat agree that the government continue to strengthen its framework for defending government networks from cyber attack, ensuring that its authorities and programs for cyber defence are modernized as technology and other relevant factors evolve. Public Safety, in collaboration with Communications Security Establishment and Treasury Board of Canada Secretariat, will continue to work together to align with the horizontal framework for cyber security to ensure that an appropriate governance structure is in place to advance cyber security policy. Responsible organizations: Public Safety, in consultation with Communications Security Establishment and Treasury Board of Canada Secretariat.
Recommendation (R2.1) To the greatest extent possible, the government: Apply Treasury Board policies relevant to cyber defence equally to departments and agencies.
Response Agreed. The Treasury Board of Canada Secretariat will review the Treasury Board policy framework to ensure that cyber defence is applied equally to departments and agencies to the greatest extent possible. This includes alignment between the scope of the *Policy on Government Security* and the *Policy on Service and Digital*. Responsible organization: Treasury Board of Canada Secretariat.
Recommendation (R2.2) To the greatest extent possible, the government: Extend Treasury Board policies relevant to cyber defence to all federal organizations, including small organizations, Crown Corporations and other federal organizations not currently subject to Treasury Board policies and directives related to cyber defence.

Response

Agreed. The Treasury Board of Canada Secretariat will undertake a review of the Treasury Board policy framework to explore and identify potential options to extend Treasury Board policies relevant to cyber defence to all federal organizations, including small organizations, Crown Corporations, and other federal organizations not currently subject to Treasury Board policies and directives related to cyber defence. This review will take into consideration the *Financial Administration Act* and the authorities under that Act, as well as any legal considerations.

Responsible organization: Treasury Board of Canada Secretariat.

Recommendation (R2.3)

To the greatest extent possible, the government:

Extend advanced cyber defence services, notably Enterprise Internet Service of Shared Services Canada and the cyber defense sensors of the Communication Security Establishment, to all federal organizations.

Response

Agreed. Treasury Board of Canada Secretariat, in consultation with Shared Services Canada and Communications Security Establishment agree that the government should extend advanced cyber defence services, notably the Enterprise Internet Service of Shared Services Canada and the cyber defense sensors of the Communication Security Establishment, to all federal organizations to the greatest extent possible.

Treasury Board of Canada Secretariat will continue to strengthen cyber defence measures as part of the updates to the Policy on Service and Digital, specifically through the mandatory procedures outlined under Appendix G: Standard on Enterprise IT Service Common Configurations of the *Directive on Service and Digital* which will be published in Early 2022.

Shared Services Canada, in consultation with Treasury Board of Canada Secretariat and Communications Security Establishment, and as part of a funded study, is evaluating the current posture of small departments and agencies (SDAs) that have not adopted the Enterprise Internet Service of Shared Services Canada. The goal of the evaluation is to produce a costed business case outlining the funding necessary to migrate SDAs to the Enterprise Internet Service of Shared Services Canada, eliminate the use of non- Shared Services Canada managed internet services, and provision other enterprise services (including the cyber defense sensors of the Communication Security Establishment), which will help to improve the security posture of SDAs and reduce the threat exposure of the government's enterprise networks.

Communications Security Establishment, in consultation with Treasury Board of Canada Secretariat, will explore options to extend the cyber defense sensors of the Communications Security Establishment to all federal organizations.

Responsible organizations: Treasury Board of Canada Secretariat, in consultation with Shared Services Canada and Communications Security Establishment.

Annex A – List of Witnesses

Communications Security Establishment

- Head, Canadian Centre for Cyber Security
- Associate Head, Canadian Centre for Cyber Security
- Director General, Cyber Defence Capabilities, Canadian Centre for Cyber Security
- Director General, Incident Management and Threat Mitigation, Canadian Centre for Cyber Security
- Director General, Policy, Disclosure and Review
- Director General, Program Evolution, Canadian Centre for Cyber Security
- Director, Incident Management and Operational Coordination, Canadian Centre for Cyber Security
- Director, Policy and Review

Treasury Board of Canada Secretariat

- Acting Chief Information Officer of Canada
- Acting Executive Director for Cyber Security