National Security and Intelligence Committee of Parliamentarians

Annual Report 2018

(Revised version pursuant to subsection 21(5) of the *NSICOP Act*)

Submitted to the Prime Minister on December 21, 2018 pursuant to subsection 21(2) of the *National Security and Intelligence Committee of Parliamentarians Act*

Canada

Ottawa, ON

National Security and Intelligence Committee of Parliamentarians

Annual Report 2018 (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP100 (Print)
CP100E-PDF (Online)
ISSN 2562-5101 (Print)
ISSN 2562-511X (Online)

ANNUAL REPORT 2018

The National Security and Intelligence Committee of Parliamentarians

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

April 2019

Revisions

Consistent with sub-section 21(1) of the *National Security and Intelligence Committee of Parliamentarians Act* (NSICOP Act), the Committee must submit an annual report to the Prime Minister. Consistent with subsection 21(5) of the 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 annual 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 report provided to the Prime Minister on 21 December 2018. Revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national defence, national security 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. ***]

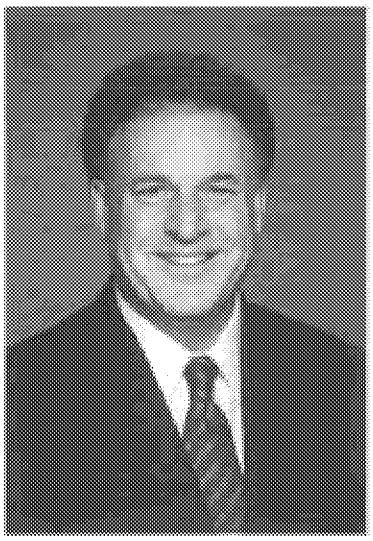


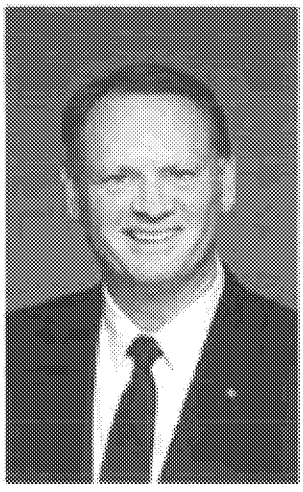
Image credit: ©House of Commons Collection, Ottawa

Dedication

The National Security and Intelligence Committee of Parliamentarians dedicates its first Annual Report to the memory of Gordon Brown, Member of Parliament for Leeds–Grenville–Thousand Islands and Rideau Lakes. He was a good colleague and a dear friend. His commitment to public service continues to inspire us.

Chair's Message

Ottawa, ON – December 21, 2018



It is my honour to submit the first Annual Report of the National Security and Intelligence Committee of Parliamentarians.

The Annual Report marks the first time that Canada has had a committee of Parliamentarians cleared to examine issues of national security and intelligence. This Committee takes that responsibility very seriously. In our first year, we have conducted 54 meetings totaling 220 hours as part of our commitment to understanding the roles and responsibilities of Canada's security and intelligence organizations and the issues that affect them.

I am proud of the dedication and engagement of the members – from all parties and from both the House of Commons and Senate – who have shown great commitment and collegiality. Our work has demonstrated that there are issues which are beyond partisanship – accountability, the security of Canada, and the protection of our democratic rights and freedoms.

In the coming year, the Committee intends to maintain an ambitious pace. We will continue to meet with departments and agencies, with our allied counterparts, with academics and experts, and with civil rights groups to ensure that our work continues to be relevant and well-informed. As we review national security and intelligence activities and organizations, we hope that our findings and recommendations strengthen the accountability and effectiveness of Canada's security and intelligence community.

Finally, I encourage Canadians to read our report and the many excellent documents produced by the departments and agencies responsible for the security of Canada. While Parliamentarians, review bodies and government officials work on behalf of all Canadians, there is no substitute for a citizenry that is well-informed of the risks facing Canada and the measures in place to address them. I hope that the work of this Committee contributes to better informing debate on issues that are of fundamental importance to Canadians.

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

THE NATIONAL SECURITY AND INTELLIGENCE COMMITTEE OF PARLIAMENTARIANS

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

Mr. Gordon Brown, M.P.
(Deceased May 2nd, 2018)

The Hon. Tony Clement, P.C., M.P.
(Resigned November 7th, 2018)

The Hon. Percy Downe, Senator

Mr. Emmanuel Dubourg, M.P.

The Hon. Hedy Fry, P.C. M.P.

Ms. Gudie Hutchings, M.P.

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

Mr. Murray Rankin, M.P.

Ms. Brenda Shanahan, M.P.

The Hon. Vernon White, Senator

National Security and Intelligence Committee of Parliamentarians

Chair

Comité des parlementaires sur la sécurité nationale et le renseignement

Président

April 8, 2019

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 present you with its Annual Report for 2018. The report includes the two substantive reviews completed by the Committee in its first year of activity, notably on the Government of Canada's process to establish its intelligence priorities, and the intelligence activities of the Department of National Defence and the Canadian Armed Forces. The Committee makes eleven findings and seven recommendations.

Consistent with subsection 21(5) of the *National Security and Intelligence Committee of Parliamentarians Act*, the report was revised to remove content deemed injurious to national security, international relations, national defence, and information subject to solicitor-client privilege.

Yours sincerely,

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

TABLE OF CONTENTS

Introduction

1. The National Security and Intelligence Committee of Parliamentarians (NSICOP or "the Committee") is pleased to present the Prime Minister with its first Annual Report. This past year ushered in a new approach to review and accountability in what is termed Canada's "security and intelligence community." Like our closest allies,[1] Canada now has an all-party committee composed of members from both houses of Parliament, cleared to view the most sensitive material and with a mandate to conduct wide-ranging reviews of national security and intelligence across the government. The Committee had a full agenda in its first year. It held an extensive series of information meetings and site visits with the core departments and agencies of the community, conducted a special review in April and May, and completed two separate reviews under its legislated mandate. It also initiated relationships with other review bodies in Canada and among its allies, and started to engage the academic and civil liberties communities. Throughout this period, the security and intelligence community has been supportive and generous with its time and expertise. The Committee looks forward to continuing its work in the years ahead.

2. The Committee drafted the Annual Report with a number of key objectives in mind. First, it believes that the recommendations and findings stemming from its review should serve to strengthen the many organizations that comprise Canada's security and intelligence community, in both effectiveness and accountability. The Committee also seeks to inform Canadians and Parliamentarians of the activities of those organizations and of the security and intelligence community overall. Finally, it hopes to inform democratic debate on the interplay among issues of security, rights and freedoms.

3. To situate the work of the Committee, this Annual Report begins by describing the security and intelligence review apparatus in Canada. This first chapter provides a historical summary of the origins of the Committee and its mandate. It also describes the factors that the Committee considers when deciding what it will review. Finally, it provides a description of the Committee's activities in its first year.

4. Chapter 2 provides a functional and practical description of the security and intelligence community, including its key activities and relationships that work to keep Canadians safe and to promote Canadian interests.

5. Chapter 3 presents the Committee's review of the Government of Canada's process for setting intelligence priorities. This process is fundamental to democratic accountability. Through it, Cabinet provides direction on intelligence priorities to the community as a whole, and ministers direct their respective departments and agencies. As such, the priority-setting process provides the governance and prescriptive elements for the collection and assessment of intelligence by the security and intelligence community in support of government policy objectives and operations. The Committee undertook a

[1] The "Five Eyes" (Canada, the United States, the United Kingdom, Australia and New Zealand).

review of this process under paragraph 8(1)(*a*) of the *National Security and Intelligence Committee of Parliamentarians Act* (*NSICOP Act*).

6. Chapter 4 details the Committee's review of the intelligence activities of the Department of National Defence and the Canadian Armed Forces (DND/CAF). Although this intelligence program is the single largest in Canada and involves a number of different intelligence collection activities, it is not specified in legislation and the Canadian public is largely unaware of it. Until the creation of NSICOP, the DND/CAF intelligence program had not been subject to external review. The introduction of review is timely, however, as the program is forecast to grow under Canada's "Strong, Secure, Engaged" defence policy. Given the size and scope of this program, the Committee conducted a focused review of the structure and authorities of DND/CAF intelligence activities under paragraph 8(1)(b) of the *NSICOP Act*.

7. The closing chapter of the Annual Report provides some concluding thoughts on the Committee's experience in its first year of operation and briefly describes the Committee's plans for 2019.

Chapter 1: Review in Canada and NSICOP's Mandate

What is review and who conducts it in Canada?

8. Security and intelligence review plays an important role in a parliamentary democracy. By their very nature, security and intelligence organizations must at times operate in secret to protect the sources and methods required to obtain intelligence and fulfill their mandates. They also have legal powers that may implicate the privacy and civil rights of Canadians. It is therefore essential that mechanisms be in place to ensure that these organizations operate effectively and in full compliance with the law. Parliament plays a foundational role by creating the legislative framework under which security and intelligence organizations work. Ministers are accountable for the oversight of those organizations, including the implementation of policy and initiatives, the authorization of certain activities, and the development of proposals to advance the government's agenda and address challenges. Dedicated review bodies are responsible for the post-facto examination of an organization's compliance with legislation and ministerial direction, and investigate public complaints. The courts also play a role in issuing judicial warrants and determining the legality of investigations through judicial proceedings.

9. Specialized review in Canada has traditionally focused on specific organizations. Three review bodies currently fulfill this role:

- The Security Intelligence Review Committee (SIRC) is an independent, external review body that reports on the performance and operations of the Canadian Security Intelligence Service (CSIS) and investigates public complaints.[2] Both SIRC and CSIS were created in 1984 under the *CSIS Act* following the recommendations of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (the McDonald Commission).
- The Office of the Communications Security Establishment Commissioner (OCSEC) was initially created in 1996 under Part II of the *Inquiries Act* to review the legality of the work of the Communications Security Establishment (CSE). In the fall of 2001, Parliament passed the *Anti-terrorism Act*, which formally codified CSE and OCSEC within the *National Defence Act*. OCSEC provides independent, external review of CSE activities to determine legal compliance and whether satisfactory measures are in place to protect the privacy of Canadians, and investigates complaints.[3]
- Distinct and independent from the Royal Canadian Mounted Police (RCMP), the Civilian Review and Complaints Commission for the RCMP is an agency that reviews specified activities for compliance, receives complaints from the public about the conduct of RCMP members, conducts reviews when complainants are not satisfied with the RCMP's handling of their

[2] Security Intelligence Review Committee, "Overview." Retrieved from: www.sirc-csars.gc.ca/index-eng.html.
[3] Office of the Communications Security Establishment Commissioner, "Overview." Retrieved from: www.ocsec-bccst.gc.ca/en.

complaints, and initiates complaints and investigations into RCMP conduct.[4] Its authorities were expanded in 2013 when it replaced the Commission for Public Complaints Against the RCMP.

10. As a whole, these review bodies are staffed with a range of experts who have access to all the information, operations, and personnel of the organizations they review, with few exceptions. Over time, their reports and recommendations have helped CSIS, CSE, and the RCMP to improve their operations, increased the confidence of Canadians that the activities of those organizations complied with the law, and identified issues for consideration by ministers or Parliament. Over SIRC's 30 years of existence, for example, it has developed expertise on and knowledge of CSIS and CSIS operations that have strengthened national security accountability in Canada.

11. Beyond these specialized review bodies, other federal institutions have the authority to examine security and intelligence organizations in Canada. As part of the responsibilities and obligations of the legislative branch of government, parliamentary standing committees are empowered to review the policies, programs, and expenditure plans of government departments and agencies. However, these committees do not conduct systematic and dedicated reviews of the security and intelligence community, nor do members of parliamentary standing committees possess the necessary security clearances to examine classified information.

12. Officers of Parliament also conduct reviews of federal departments and agencies. For example, the Office of the Auditor General conducts financial and performance audits of some 100 departments and agencies, 40 Crown corporations, the territorial governments, and numerous territorial corporations on a broad range of government activities.[5] Similarly, the Privacy Commissioner conducts audits of federal institutions subject to the *Privacy Act* to protect and promote the privacy rights of individuals.[6] These organizations conduct audits of members of the security and intelligence community, but their scope of responsibility is very broad and their reviews focus on the relatively specialized areas of their mandates.

13. Beyond these permanent structures, the federal *Inquiries Act* also provides a statutory framework for the government to initiate a review of a specific event, challenge or department. Part I of this Act allows the government to empower a commissioner to conduct public inquiries on any matter connected with the good government of Canada. Departmental investigations conducted under Part II grant any minister presiding over a department in the federal public administration with the ability to appoint, under the authority of the Governor in Council, a commissioner to investigate and report on the state and management of the business of a department. The more recent landmark inquiries into

[4] Civilian Review and Complaints Commission for the RCMP, "About Us." Retrieved from: www.crcc-ccetp.gc.ca/en/about-us.
[5] Office of the Auditor General of Canada, "What We Do." Retrieved from: www.oag-bvg.gc.ca/internet/English/au_fs_e_371.html.
[6] Office of the Privacy Commissioner of Canada, "Audits." Retrieved from: www.priv.gc.ca/en/opc-actions-and-decisions/audits/.

the activities of the Canadian security and intelligence community were conducted under this Act in the mid-2000s, notably the following:

- In 2006, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (the O'Connor Commission) examined how the actions of Canadian officials contributed to the apprehension, extra-judicial transfer and subsequent torture of Mr. Arar in Syria. In the Factual Inquiry, Justice O'Connor provided a series of recommendations that focused on the actions of Canadian officials. In its Policy Review, the Commission recommended an independent review mechanism for the national security activities of the RCMP and review mechanisms for other departments.
- In October 2008, Justice Iacobucci issued the report on the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nureddin. While the Inquiry did not make recommendations, Justice Iacobucci noted that the activities of the RCMP and CSIS indirectly contributed to the detention and mistreatment of the three individuals by Syrian and Egyptian officials.
- In 2010, the Honourable John Major completed the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (the Major Commission). Its key recommendations focused on enhancements to the role of the National Security Advisor, improved information sharing across organizations, and the modernization of the *CSIS Act*.

What was missing?

14. Review in Canada previously centred on specific organizations and did not contemplate wider issues. The specialized review apparatus in Canada focused solely on the specific activities of CSIS, CSE, and the RCMP. No entity previously had the authority, mandate or capacity to follow the trail of an activity or investigate a case across those organizations, nor across the broader federal government to other organizations with security and intelligence responsibilities. While the various security and intelligence organizations form a community within the federal bureaucracy, no commensurate review function was in place to examine issues or functions with an interdepartmental lens. Furthermore, specialized review bodies primarily examined the legality of activities, but could not conduct strategic or framework reviews of the security and intelligence community as a whole.

15. Review did not include a specialized parliamentary body or a body of Parliamentarians. From an international perspective, Canada's closest allies have long had parliamentary or legislative review bodies for their respective national security and intelligence organizations. In France, la Délégation parlementaire au renseignement is a bicameral committee of eight members responsible for monitoring the French intelligence services. It can take testimony from the Prime Minister, ministers and heads of agencies, is authorized to receive classified information, and must produce an annual report on its activities, observations, and recommendations. In Westminster-style democracies, these review bodies have narrow mandates. For example, the Intelligence and Security Committee of Parliament in the United Kingdom is empowered to review three specific agencies: the Security Service (MI5), the Secret Intelligence Service (MI6), and the Government Communications Headquarters (GCHQ). Any review beyond these three agencies requires a memorandum of understanding between the Committee and the Prime Minister. In Australia, the Parliamentary Joint Committee on Intelligence and Security may review the administration and expenditures of certain agencies and the functions of the Australian Federal Police's performance related to terrorism. This Australian committee also conducts statutory reviews of legislation. In New Zealand, the Prime Minister chairs the Intelligence and Security Committee, which examines the policy, administration, and expenditures of each intelligence and security agency. It can also review legislation referred to it by the House of Representatives. The role of legislative bodies in the United States is considerably different from Westminster-style accountability and review functions. For example, the House Permanent Select Committee on Intelligence provides oversight of the intelligence community, studies intelligence-related activities, and examines legislative proposals, while the U.S. Senate Select Committee on Intelligence conducts hearings and reviews of intelligence activities, and provides funding levels and regular oversight.

What is NSICOP's mandate and does it address some of the review gaps?

16. The idea of national security and intelligence review by a committee of Parliamentarians has been raised at various times in Canada since the early 1980s. In its 1981 report, the McDonald Commission originally recommended the establishment of a Joint Committee of Parliament on Security and Intelligence (this recommendation was not implemented). In 2005, the Government introduced a bill to establish a National Security Committee of Parliamentarians, but it died on the *Order Paper* five days later. The idea was subsequently revived through private members' bills introduced in the House of Commons on a number of occasions, but never progressed beyond first reading.

17. On June 16, 2016, the Leader of the Government in the House of Commons introduced Bill C-22, *An Act to establish the National Security and Intelligence Committee of Parliamentarians*, and to make consequential amendments to certain acts. In speaking to the principles and motivation of establishing NSICOP, the Minister of Public Safety and Emergency Preparedness stated that this initiative was a cornerstone of the Government's approach to ensuring that Canada's national security framework is working effectively to keep Canadians safe while protecting their rights and freedoms.[7] In announcing the appointment of NSICOP members in 2017, the Prime Minister stated:

> The creation of a strong, accountable, and multi-party committee of dedicated parliamentarians will help us ensure that our national security agencies continue to keep Canadians safe in a way that also safeguards our values, rights, and freedoms. This independent group will help strengthen the accountability of our national security and intelligence work. In our system of responsible government, there is no substitute for scrutiny by parliamentarians.[8]

18. On June 22, 2017, the *National Security and Intelligence Committee of Parliamentarians Act* (*NSICOP Act*) received Royal Assent.[9] In accordance with section 8 of the Act, the Committee has a broad mandate to review:

- the legislative, regulatory, policy, administrative, and financial framework for national security and intelligence;

[7] House of Commons, Standing Committee on Public Safety and National Security, *Evidence of Proceedings*, 1st Session, 42nd Parliament, Meeting 40, 2016, p. 2. Retrieved from: www.ourcommons.ca/Content/Committee/421/SECU/Evidence/EV8564344/SECUEV40-E.PDF.

[8] Prime Minister of Canada, "Prime Minister announces new National Security and Intelligence Committee of Parliamentarians," News release, November 6, 2016. Retrieved from: https://pm.gc.ca/eng/news/2017/11/06/prime-minister-announces-new-national-security-and-intelligence-committee.

[9] *National Security and Intelligence Committee of Parliamentarians Act*, S.C. 2017, c. 15. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/N-16.6/FullText.html.

- any activity carried out by a department that relates to national security or intelligence, unless the activity is an ongoing operation and the appropriate minister determines that the review would be injurious to national security; and
- any matter relating to national security or intelligence that a minister of the Crown refers to NSICOP.

19. On November 6, 2017, the Prime Minister appointed the inaugural 11 members of NSICOP, including the Chair. The members come from both houses of Parliament, and all hold the highest security clearances, are permanently bound to secrecy under the *Security of Information Act*, and are subject to security requirements in the National Security and Intelligence Committee of Parliamentarians Regulations. Members swear an oath or solemn affirmation that they will obey and uphold the laws of Canada, not communicate or inappropriately use information obtained in confidence as part of their responsibilities on the Committee, and may not invoke their parliamentary privileges. On this basis, members are able to receive classified briefings and materials related to the conduct of the Committee's work.

20. The *NSICOP Act* gives the Committee significant but not unfettered access to information. Under section 13 of the Act, it is entitled to have access to any information that is under the control of a department related to the fulfillment of the Committee's mandate. This includes information protected by litigation privilege or by solicitor-client privilege. However, section 14 of the Act lists four exceptions to the Committee's right of access to information:

- confidences of the Queen's Privy Council (i.e., Cabinet Confidences);
- information related to subsection 11(1) of the *Witness Protection Program Act*, specifically pertaining to the disclosure of information associated with the identity of a protected person;
- the identity of confidential sources of information, intelligence or assistance; and
- information related to an ongoing investigation carried out by a law enforcement agency that may lead to a prosecution.

In addition, ministers of the Crown may refuse to provide the Committee with information on the grounds that it constitutes "special operational information," as defined in subsection 8(1) of the *Security of Information Act*, and the provision of the information would be injurious to national security.[10] This includes a wide range of information that the Government of Canada is taking measures to safeguard, the content of military plans for operations, or the subject of a covert investigation.

21. Ministers may also determine that an entire proposed NSICOP review involves an ongoing investigation and is injurious to national security. In that case, the minister must inform the Committee of his or her decision and the reasons for it. Should the Minister determine at a later date that the

[10] *Security of Information Act*, R.S.C. 1985, c. O-5. Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/O-5/FullText.html.

review proposal is no longer injurious or that the activity is no longer ongoing, he or she must inform the Committee that the review may be conducted.

22. Under the *NSICOP Act*, the Committee must produce an annual report that includes the reviews conducted in the preceding year. This report contains the Committee's findings and recommendations, as well as the number of times in the preceding year that a minister determined that a review under paragraph 8(1)(*b*) would be injurious to national security or refused to provide information because, in the minister's opinion, the information constituted special operational information and that providing it would be injurious to national security. The Committee may also complete a special report on any matter related to its mandate, at any time, and submit such a report to the Prime Minister. The Committee completed a Special Report on the Prime Minister's February 2018 trip to India.

23. As part of the submission of reports to the Prime Minister, the *NSICOP Act* provides the government with an ability to protect certain information from public disclosure. The Prime Minister may direct the Committee to revise a report so that it does not contain information the disclosure of which would be injurious to national security, national defence or international relations, or is information that is protected by litigation privilege or by solicitor-client privilege. An example of the criteria for each of these elements can be found in the *Canada Evidence Act*. Along with jurisprudence and legal precedent, the *Canada Evidence Act* provides the framework for the detailed redaction of such confidential information.

24. In the discharge of its responsibilities, the Committee receives support from its Secretariat. The main functions of the Secretariat are ensuring that members receive timely access to relevant, classified information, and expert advice in the conduct of reviews and the development of reports. The Secretariat has an annual budget of approximately $3.5 million and funding for 10 full-time employees who are appointed in accordance with the *Public Service Employment Act*. The Secretariat is staffed with officials, most of whom have experience working across the various departments and agencies of the security and intelligence community.

25. The Committee's review mandate is both consistent with the existing review approach and unprecedented in the Canadian context. The mandate is consistent with existing review in Canada in that it is based on analysis of the activities of organizations, and with the principal objective of review, which is to improve the functioning of the security and intelligence community. For the Committee, that means identifying where gaps may exist in legislation, policies, or governance; strengthening ministerial accountability; and improving transparency. It also means that the Committee will work to help Canadians better understand the roles and responsibilities of the organizations responsible for serving them and to better understand the interplay between security and the rights and civil liberties of Canadians.

26. On the other hand, the Committee's mandate is unprecedented in that it allows Parliamentarians to look at issues from a government-wide perspective and to make findings and recommendations that may benefit individual organizations, improve the interaction among organizations, or strengthen the

security and intelligence community overall. The Committee has therefore structured its own approach to review on the valuable precedent set by SIRC and OCSEC, and on the experience of relevant counterpart organizations among our close international allies.[11]

[11] Most notably the Five Eyes countries.

What is NSICOP's role and how does it operate?

27. The security and intelligence landscape is in constant evolution. Organizations must respond to an ever-changing threat landscape. Governments implement legislative changes or budgetary measures to enhance or change the scope of national security and intelligence activities. Jurisprudence causes organizations to adjust how they conduct their respective operations. Specialized review bodies provide recommendations that improve the work of the specific organizations and their compliance with the law. It is in this context that the Committee will contribute to the evolution of national security and intelligence activities in Canada.

28. The Committee views itself as an important component of accountability within the security and intelligence community. Ministers remain responsible for the activities of the departments and agencies within their portfolio (their role is **oversight** rather than review), but they benefit from independent whole-of-government review of national security and intelligence. The Committee's mandate strengthens the accountability by enabling Parliamentarians to scrutinize the necessarily secret activities of the state and to hold the government to account on the interplay between security and the rights of all Canadians. The Committee expects its role will cultivate and maintain the public's trust in the activities of their institutions, in accordance with the rule of law and responsible government.

29. The role of the Committee is compatible with the three existing review bodies and will become more complementary with the anticipated evolution of the review landscape in Canada under the proposed components of Bill C-59, *An Act Respecting National Security Matters*. The Bill would establish two new accountability structures to replace SIRC and OCSEC: the National Security and Intelligence Review Agency (NSIRA) and the Intelligence Commissioner. Under the proposed legislation:

- NSIRA would have a mandate to review any activity carried out by CSIS and CSE, any activity carried out by a department related to national security or intelligence, and any matter related to national security or intelligence that is referred to it by a minister. NSIRA would also investigate complaints against CSIS, CSE, and, if it relates to national security, the RCMP. Each calendar year, NSIRA would be obligated to review at least one aspect of CSIS's performance in taking measures to reduce threats to the security of Canada, the disclosure of information under the *Security of Canada Information Disclosure Act*, and the implementation of significant aspects of every new or modified ministerial direction. In the course of its reviews, NSIRA may make findings and recommendations, including those relating to a department's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of a department's exercise of powers.
- The Intelligence Commissioner would have the responsibility to review and approve ministerial authorizations for certain activities conducted by CSIS and CSE, including in the areas of foreign intelligence, cybersecurity, and datasets.

30. Should Bill C-59 pass in its present form (as of December 2018), the establishment of NSIRA will provide greater review symmetry within the national security and intelligence community. It will

balance the Committee's broad framework reviews and the scrutiny of Parliamentarians, with the specific activity and compliance reviews undertaken by NSIRA. This review apparatus will be equipped to make organizational and community-wide findings and recommendations on functionality, efficiency, and legality. Coordination and collaboration between NSICOP and NSIRA will be essential to avoid duplication and maximize the effectiveness of review.

31. The Committee believes in the importance of leveraging the expertise of other entities involved in assessing the activities of the federal bureaucracy, most notably the Auditor General and the Privacy Commissioner, as well as academics. The Committee intends to explore opportunities for cooperation in the years ahead.

32. The Committee believes in the informed and non-partisan review of national security and intelligence. Members of the Committee agree to NSICOP's schedule and agenda, and any member can propose a review for consideration. The Committee meets *in camera* at a secure location to ensure its discussions are confidential, non-partisan, and free flowing. Committee members actively engage in the consideration of materials, the preparation of review reports, and briefings from the security and intelligence community. The Chair's role consists of building consensus, providing guidance to the Committee in its deliberations, and working closely with the Secretariat, including to develop review proposals for Committee consideration. The Chair also communicates terms of reference for specific reviews to responsible ministers, and provides the Committee's reports to the Prime Minister.

How does NSICOP decide what to review?

33. The work of the security and intelligence community offers a broad range of topics worthy of review. How does the Committee decide what to examine? For the purpose of its reviews, the Committee has adopted working definitions of both "national security" and "intelligence." For the Committee to take an interest in a security issue, it should involve at least one of the core members of the security and intelligence community (see Table 1) and be national in character, understood as relating to threats to the security of Canada as defined in the *CSIS Act*, or criminality of national scope or gravity. In the area of intelligence, the issue should principally involve the use of clandestine, covert, or privileged sources or methods (in short, areas where the rights of Canadians could be significantly affected or where there are significant risks to the government) and involve at least one core member of the security and intelligence community. As practical examples, these working definitions would permit the review of terrorism investigations (a national issue implicating CSIS, the RCMP, and other federal organizations), but not gang violence (primarily the responsibility of provinces, territories, and municipalities). The Committee may also agree to review a matter referred to it by a minister, consistent with paragraph 8(1)(*c*) of the *NSICOP Act*.

34. As the Committee began its review work in the spring of 2018, it considered the breadth of issues facing the security and intelligence community. Its deliberations were informed by visits to the core departments and agencies and its engagement with their officials. It tried to determine where its reviews could add the greatest value. Aside from the working definitions outlined above, the Committee considered a number of criteria to inform its decisions. With respect to the activities of an individual organization, it considered:

- whether the organization was previously subject to review;
- the extent of its security or intelligence activities, and the degree to which they were known; and,
- whether the activities were governed by specific legislation or formal government direction (for example, an order in council).

The answers to these questions guided the Committee's assessment of the possible risks associated with the activities of an organization.

35. Its deliberations on potential reviews were informed by other considerations. These included:

- the extent to which an activity or issue implicated the privacy or democratic rights of Canadians;
- the extent to which an activity or issue affected Canadian alliances or foreign relations;
- whether there was a high level of public interest in the activity or issue;
- whether the activity or issue affected Canada's sovereignty or the integrity of its institutions, economy or society; and
- whether Parliament or another review body had previously examined the activity or issue.

36. Based on its considerations, the Committee decided to conduct a review under each of its first two mandates: a framework review under paragraph 8(1)(*a*) of the *NSICOP Act* and an activity review under paragraph 8(1)(*b*). **For its framework review**, the Committee chose to examine how intelligence priorities are established. In the Committee's interactions with senior officials from the security and intelligence community, it became clear that the process for setting intelligence priorities was a foundational part of ensuring ministerial accountability, addressing risk in the community, allocating resources, and governing the community. The Committee believed that a review of this important process would provide greater insight into how the various security and intelligence organizations operate as a community. This review is detailed in chapter 3.

37. **For its activity review**, the Committee chose to review the intelligence activities of the Department of National Defence and the Canadian Armed Forces (DND/CAF). As it learned about the security and intelligence community, the Committee was struck by the relative size of the DND/CAF intelligence program (the single largest intelligence program in Canada, measured by personnel, and the second largest budget) and the breadth of its activities. Unlike CSIS, CSE, or the RCMP, defence intelligence activities are relatively unknown in the public realm, are not specified in legislation and, until the creation of NSICOP, were not subject to external review. With the expected growth in DND/CAF intelligence capabilities described in the new "Strong, Secure, Engaged" defence policy, the Committee decided it was an appropriate time to review the structure and authorities of the DND/CAF intelligence program as a potential starting point for future reviews. This review is detailed in chapter 4.

Beyond the annual reviews, what else has NSICOP done in its inaugural year?

38. In preparing for its formal review activities, the Committee engaged with the security and intelligence community in the months following its creation. Between December 2017 and December 2018, the Committee held 54 meetings, site visits, and hearings for a total of 220 meeting-hours, representing an average of 4 hours per meeting. The Committee heard from over 60 witnesses.

39. The Privy Council Office (PCO) provided a preliminary overview of the national security and intelligence community and national security threats facing Canada. It also briefed the Committee on security procedures, requirements and regulations associated with managing classified material. Following the appointment of the Secretariat's Executive Director in December 2017, the Secretariat took over from PCO in supporting the Committee. The Secretariat facilitated a series of site visits in February, March, and April to the core national security and intelligence organizations. These included the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency, the Department of National Defence / Canadian Armed Forces (DND/CAF), Global Affairs Canada, and the Integrated Terrorism Assessment Centre. These visits permitted Committee members to further refine their understanding of the mandates and activities of the community. During March and April, the Committee considered several review proposals before selecting the two substantive reviews discussed in chapters 3 and 4.

40. The Committee held several outreach meetings with key departments and agencies. This included Public Safety Canada to discuss its roles and responsibilities, Treasury Board Secretariat to learn about funding of the security and intelligence community in Canada, and PCO to obtain an overview of the process for setting intelligence priorities. The Committee received a briefing from the Privacy Commissioner of Canada on his mandate and his experiences with reviewing the security and intelligence community in Canada. The Committee also met with academics, experts, and several civil liberties groups on the interplay between rights and security.

41. On April 5, 2018, the Committee decided to conduct a special review of certain allegations surrounding the visit by the Prime Minister to India in February 2018. Those allegations related to foreign interference in Canadian political affairs, risks to the security of the Prime Minister, and inappropriate use of intelligence. The Committee made its decision after careful consideration of the relevance of the issue to its mandate and after the Minister of Public Safety and Emergency Preparedness and, separately, the Senate had indicated that the issue should be addressed by NSICOP.[12]

[12] Beverly Thomson, "Goodale Discusses Jaspal Atwal Affair," News report, CTV News Channel, March 1, 2018. Retrieved from: www.ctvnews.ca/video?clipId=1337949&playlistId=1.3824217&binId=1.810401&playlistPageNum=1&binPageNum=1. The Committee considered the Senate of Canada's amended motion from March 2018 stating that NSICOP may be an appropriate forum to review the security and intelligence operating procedures in relation to diplomatic and foreign visits involving the Government of Canada. The full text of the motion (No. 309) can be retrieved from the

After April 20, when the Committee received the information it had requested, the Committee considered an interim report from its Secretariat, conducted hearings with senior officials from four government organizations, and completed the drafting and review of its final report. The report made a number of findings and recommendations. In October, the Committee held further deliberations on the report and provided an updated version to the Prime Minister on October 12. The declassified version of that report was tabled in Parliament on December 3rd, 2018.

42. From June to October 2018, the Committee focused on completing its two substantive reviews and finalizing its first annual report. It considered interim reports and held briefings and hearings with senior officials from CSE, CSIS, DND/CAF, PCO, Global Affairs Canada, the Integrated Terrorism Assessment Centre, and Immigration, Refugees and Citizenship Canada. As required in the *NSICOP Act*, the Committee notes that no minister exercised her or his legislative authority to refuse to provide information to NSICOP in the preceding year and no minister determined that a review was injurious to national security. It also notes that the heads of CSE and CSIS each informed the Committee of decisions they made pursuant to Ministerial Direction on avoiding complicity in mistreatment by foreign entities.

43. The Committee engaged with its review counterparts. As part of its statutory obligation to coordinate its activities with existing review bodies, the Committee and its Secretariat met with SIRC and OCSEC to discuss ongoing and planned reviews. In April, several Committee members travelled to Washington, D.C., to meet with the Australian Parliamentary Joint Committee on Intelligence and Security, which was there on separate business, to discuss that organization's review activities. While in Washington, the Committee also received a presentation by a former U.S. Under Secretary for Intelligence and Analysis at the Department of Homeland Security on oversight of the U.S. intelligence community. In October, the Committee hosted the U.K.'s Intelligence and Security Committee for meetings in Ottawa, building on exchanges between the two committees' secretariats.

44. The Committee is grateful to the Office of the CSE Commissioner for supporting the Committee's day-to-day work by providing space for Secretariat staff in the early months of 2018 and secure facilities for the Committee to hold its meetings until the Secretariat moved to its permanent facilities in September 2018. The Committee thanks officials from PCO for assisting the Committee in initiating its activities. Finally, the Committee thanks the House of Commons for its assistance with the development and hosting of NSICOP's website. The Committee's ability to inform Canadians is essential for the successful fulfillment of its mandate.

Senate's Order of Business for March 29, 2018:
https://sencanada.ca/en/Content/Sen/Chamber/421/OrderPaper/192op_2018-03-29-e.

Chapter 2: A Functional Overview of the Security and Intelligence Community

What is national security and intelligence?

45. NSICOP has a mandate to review issues of national security and intelligence. However, neither "national security" nor "intelligence" is defined in the *National Security and Intelligence Committee of Parliamentarians Act* (*NSICOP Act*) that established the Committee's mandate, nor are they defined in other legislation.

46. Official definitions of **national security** have changed over time. In 1979, the McDonald Commission proposed a simple definition of national security: the need to preserve Canadian territory from attack and to preserve and maintain the democratic process of government.[1] In 2004, the Government stated that national security relates to threats that have the potential to undermine the security of the state or society and that require a national response. It said that national security focused on three core interests: protecting Canada and Canadians at home and abroad; ensuring Canada is not a base for threats to its allies; and contributing to international security.[2] From this relatively narrow focus on security, the Government adopted a broader view. For example, a 2017 document provided to the Committee defined national security as "protecting the safety and security of Canada's territory, government, economy and people, and the promotion and protection of Canadian interests."[3] This latter definition is understandably broad: issues of security are deeply integrated with those of foreign affairs, trade and the economy, social issues, health, and the environment. As discussed in paragraph 33 of Chapter 1, the Committee has adopted a working definition of national security to help it determine what activity or issue it should review.

47. The definition of **intelligence**, on the other hand, has a stronger basis in law, but also suffers from some ambiguity. The Committee notes that there are many types of intelligence. In the *National Defence Act*, "foreign intelligence" is defined as:

> Information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.

Security intelligence is another type of intelligence. It is not defined in legislation, but relates to threats to the security of Canada as defined in the *CSIS Act*, specifically espionage or sabotage, foreign-influenced activities, terrorism, and the violent overthrow of the government. The Committee notes that other types of intelligence exist, including defence intelligence, criminal intelligence, and financial intelligence. There are also many **means** of collecting intelligence, such as recruiting human sources of

[1] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Security and Information*, First Report, Minister of Supply and Services Canada, Ottawa, 1979, p. 15, paragraph 38.
[2] Privy Council Office, *Securing an Open Society: Canada's National Security Policy*, 2004, p. vii. Retrieved from: http://www.publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.
[3] Privy Council Office, "What is National Security?" Document provided to the National Security and Intelligence Committee of Parliamentarians, 2017, p. 3

information (known as human intelligence), intercepting communications (known as signals intelligence or communications intelligence), and using public sources of information (known as open source intelligence). As discussed in paragraph 33 of Chapter 1, the Committee has adopted a working definition of intelligence to help it determine what activity or issue it should review.

Who belongs to the security and intelligence community?

48. A number of government organizations are responsible for keeping Canadians safe and for helping to promote Canadian interests abroad. Canada's security and intelligence community has seven core federal organizations that have mandates that are either entirely or substantially related to national security, intelligence, or both. The Committee added an eighth, the Prime Minister's National Security and Intelligence Advisor (NSIA), because of the important role the Advisor and his or her officials play in advising the Prime Minister and coordinating much of the security and intelligence community (see Table 1). Nine other organizations belong to the community, but have mandates and activities that are broader than either security or intelligence (see Table 2). These organizations have evolved over time in response to government priorities, legislative changes, and new challenges and threats. Over the past year, the Committee has visited each of the core members of the security and intelligence community and gained a better understanding of their mandates, authorities, and activities. It has also been briefed on the roles of the other organizations.

49. The *2016–2017 National Intelligence Expenditure Report* gives some idea of the size and scope of the intelligence community in Canada. This report on the resource allocation of federal departments and agencies to support the Government of Canada's intelligence priorities notes a budget of approximately *** and approximately *** full-time employees across 10 organizations.[4] By way of comparison, the Australian intelligence enterprise in 2016–2017 represented approximately CAD$2 billion and 7,000 staff spread across 10 agencies.[5] While Canada's National Intelligence Expenditure Report does not provide the total sum of costs associated with all intelligence activities, these figures do provide a useful comparison to a key ally of similar size and scope.

---

[4] Public Safety Canada, *2016–2017 National Intelligence Expenditure Report*, Submitted to the National Security and Intelligence Committee of Parliamentarians, 2018.

[5] Australia, Department of the Prime Minister and Cabinet, *2017 Independent Intelligence Review*, June 2017, p. 7. Retrieved from: https://www.pmc.gov.au/sites/default/files/publications/2017-Independent-Intelligence-Review.pdf.

National Security and Intelligence Advisor

- Advises the Prime Minister and Cabinet
- Coordinates the policy and operations of the security and intelligence community
- Provides intelligence assessments
- Provides a challenge function for the security and intelligence community

Communications Security Establishment

- Collects and reports on foreign signals intelligence
- Protects information and information infrastructures of importance to the Government of Canada
- Assists government departments

Canadian Security Intelligence Service

- Collects intelligence and advises on threats to the security of Canada
- Takes measures to reduce threats
- Collects foreign intelligence within Canada
- Conducts security assessments

Royal Canadian Mounted Police

- Investigates national security offences
- Investigates sophisticated organized crime
- Enforces federal legislation
- Takes measures to reduce threats
- Conducts threat assessments

Department of National Defence / Canadian Armed Forces

- Conducts 'full spectrum' intelligence operations to support military operations
- Collates and assesses intelligence

Global Affairs Canada

- Manages foreign policy, including international security issues
- Manages emergency response overseas
- Obtains privileged information through personnel posted abroad
- Manages foreign intelligence relationships

Canada Border Services Agency

- Ensures border integrity at ports of entry
- Uses intelligence and other data to make risk-based decisions regarding the admissibility of persons and goods to Canada

Integrated Terrorism Assessment Centre

- Analyzes terrorism threats to Canada and Canadian interests
- Recommends the National Terrorism Threat Level
- Sets terrorism threat levels against Canadian interests abroad, including special events

Table 1. Core Members of the Security and Intelligence Community

Canadian Coast Guard	Natural Resources Canada
Financial Transactions and Reports Analysis Centre of Canada	Public Health Agency of Canada
Immigration, Refugees and Citizenship Canada	Public Safety Canada
Innovation, Science and Economic Development Canada	Transport Canada
Justice Canada	

Table 2. Other Federal Departments and Agencies involved in National Security and Intelligence

50. While the security and intelligence organizations each have specific mandates and responsibilities, they share common objectives (e.g., keeping Canadians safe) and work together to achieve them. In short, they function as a community: their breadth and level of engagement is unique in government. While accountability for each of the individual departments and agencies is exercised by the responsible minister, issues of national security and intelligence have long been considered of exceptional importance and sensitivity.

51. The Prime Minister and Cabinet therefore play an important leadership and coordination role over the community as a whole. As of late August 2018, the committee responsible is the Cabinet

Committee on Canada in the World and Public Security, which is chaired by the Minister of Health. In addition, the Prime Minister has created the Incident Response Group (IRG). The IRG brings together relevant ministers and senior government leadership to coordinate federal responses to national crises or incidents elsewhere that have major implications for Canada. Prior to August 2018, the Prime Minister chaired the Cabinet Committee on Intelligence and Emergency Management, which met to consider intelligence reports and priorities, to coordinate and manage responses to public emergencies and national security incidents, and to review the state of Canadian readiness. In the past, similar functions were played by other permanent and ad hoc Cabinet committees.

52. The Prime Minister is advised by the NSIA, a senior official responsible for coordinating and providing leadership to the security and intelligence community. The NSIA regularly briefs and provides advice to the Prime Minister and other government officials on national security and intelligence issues, including for seeking the Prime Minister's concurrence to conduct particularly sensitive activities.

53. The NSIA reports to the Clerk of the Privy Council and is responsible for three organizations in the Privy Council Office: the Foreign and Defence Policy Secretariat, the Security and Intelligence Secretariat, and the Intelligence Assessment Secretariat. These Secretariats help to coordinate the operational, policy, and assessment activities of the community in the areas of foreign affairs, defence, security, and intelligence. The NSIA chairs two deputy minister-level committees, one on operations (which meets weekly) and one on intelligence assessment (which meets monthly). The NSIA co-chairs with the Deputy Minister of Public Safety a monthly deputy minister-level committee on national security. These committees are supported in turn by officials from across the community. The NSIA also leads ad-hoc meetings of officials to address significant events or crises. The office of the NSIA has no statutory basis, but relies on the authority derived from his or her position at the Privy Council Office and as a principal advisor to the Prime Minister. The biennial process to identify, approve, and implement intelligence priorities, which the NSIA coordinates, is an important mechanism to govern the community and ensure accountability to ministers and Cabinet. This issue is discussed further in chapter 3.

54. Public Safety Canada plays a coordination and leadership role in national security. The Minister of Public Safety and Emergency Preparedness is accountable for three core members of the security and intelligence community: the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and the Canada Border Services Agency. The Minister is regularly briefed on the activities of those organizations and approves a number of their operations. The department leads, coordinates, or supports several security processes, including the processes of listing terrorist entities, listing individuals on the Passenger Protect Program, and conducting national security reviews of foreign investments. In cyber security, the department works with other government departments and the private sector to mitigate cyber threats to critical infrastructure (for example, the financial system) and to promote cyber security to Canadians. The Deputy Minister of Public Safety leads a deputy minister-level committee on cyber issues, which meets as required to discuss cyber threats, operations, and policy issues.

55. The work of these organizations is vital. Every day, government employees across the country and around the world – intelligence officers, police investigators, diplomats, soldiers, and border services officers, to name a few – work to protect Canadians and to advance Canadian interests in areas

like trade and international relations. Some of these organizations use sophisticated and covert methods to conduct their work and are subject to significant levels of oversight and review, including through the courts, ministerial approvals, and independent review bodies.

56. The Committee is of the view that this work is not well understood. Canadians do not appear to have a strong understanding of the individual mandates or activities of each of the organizations of the security and intelligence community, how they work together, or the role of their review bodies. For example, recent public opinion research shows that only 3 percent of respondents could correctly identify the Communications Security Establishment (CSE) unprompted and only 37 percent said that they had previously heard about the organization.[6] Other research shows that only 3 in 10 Canadians can identify CSIS.[7] Department of National Defence and the Canadian Armed Forces (DND/CAF) public opinion research shows that only 26 percent of Canadians had some awareness of the military's activities from the past year and a half.[8] However, information on these organizations is publicly available. Each has a website which describes its roles and authorities (CSE is particularly good in this regard), and both the Security Intelligence Review Committee and the CSE Commissioner have published detailed reports on their reviews of the work of the two key organizations, CSIS and CSE, annually. There is also a wealth of academic and online resources to inform Canadians. The Committee believes that Canadians would be well served if government information were more user-friendly. More specifically, it believes that the public would benefit from information that explains how security and intelligence works and the role that government organizations play individually and in concert to protect Canadians and to advance their interests. That information should be consolidated for ease of reference and standardized for completeness.

57. There appears to be a similar lack of awareness of threats to Canada's national security. As it stands now, an interested Canadian would have to search a number of government websites to understand the most significant threats to Canada. For some threats, such as terrorism, information is readily available and regularly updated (for example, the annual Public Report on the Terrorist Threat to Canada). For other threats, such as organized crime or interference in Canadian domestic politics, information is often limited, scattered among different sources or incomplete. The Committee believes that Canadians would be equally well served if more information about threats were readily available.

---

[6] Sean Kilpatrick, "Just 3% of Canadians can name the Communications Security Establishment: Survey," Canadian Press, November 8, 2017. Retrieved from: https://www.huffingtonpost.ca/2017/11/08/just-3-of-canadians-can-name-the-communications-security-establishment-survey_a_23270492/.

[7] Canadian Security Intelligence Service, *Attitudes to the Canadian Security Intelligence Service (CSIS) – Baseline Study*, June 2018. Retrieved from: http://epe.lac-bac.gc.ca/100/200/301/pwgsc-tpsgc/por-ef/canadian_security_intelligence_service/2018/101-17-e/report.html.

[8] Murray Brewster, "Military is off the radar of most Canadians: DND poll," CBC News, July 20, 2018. Retrieved from: https://www.cbc.ca/news/politics/dnd-canadians-military-poll-1.4754083.

Keeping Canadians safe

58. The following section provides a high-level, functional overview of Canada's security and intelligence community. It does not detail the mandate, authorities, and activities of all of the community's members, with one exception (DND/CAF, described in chapter 4). Nor does it try to address the gaps noted above – the Committee believes that the ministers accountable for the departments themselves are responsible for better informing Canadians about the range of threats facing Canada and the role that certain organizations play in addressing them. Rather, the section reflects what the Committee has learned through its interaction with the security and intelligence community since its inception.

59. The Government states that its first priority is to protect the safety and security of Canadians at home and abroad. In a national security context, that involves a range of activities to detect, prevent, or disrupt threats to the security of Canada. Key members of the security and intelligence community provided the Committee with an overview of the most significant national security threats. Briefings and open source information provided to the Committee on these issues form the basis of the following functional overview.

Terrorism

60. The Privy Council Office briefed the Committee on a number of threats to Canada's national security. The first was terrorism. Over the years, there have been many terrorist threats to Canada and its allies. The terrorist threats facing Canada now are elaborated in the 2017 Public Report on the Terrorist Threat to Canada.[9] The report states that violent extremists inspired by Al-Qaida and Daesh continue to be the main terrorist threat to Canada and that these groups are able to communicate with ease with the use of social media and encryption technologies. According to the Integrated Terrorism Assessment Centre, the national threat level for terrorist attacks is currently medium, meaning that a violent act of terrorism could occur and that additional measures are in place to keep Canadians safe.[10] The threat level was set following a 2014 speech by Daesh encouraging attacks in Canada. The October 2014 terrorist attacks in St-Jean-sur-Richelieu and in downtown Ottawa occurred shortly thereafter and the threat level has not changed since. The Integrated Terrorism Assessment Centre assigns different threat levels to each of Canada's major municipalities and to different types of transportation (for example, rail or commercial air); ***. Threat level assessments provide government officials and law enforcement agencies with details on risks and vulnerabilities to inform mitigation strategies and security postures.

61. The federal organizations with primary responsibility for investigating, preventing, or disrupting terrorist threats are CSIS and the RCMP. As an intelligence organization, CSIS collects and analyzes

[9] Public Safety Canada, *2017 Public Report on the Terrorist Threat to Canada*, 2017. Retrieved from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pblc-rprt-trrrst-thrt-cnd-2017/pblc-rprt-trrrst-thrt-cnd-2017-en.pdf. The 2018 report was published after this report was finalized.
[10] Integrated Terrorism Assessment Centre, *Canada's National Terrorism Threat Levels*, 2018. Retrieved from: https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html.

information for the purpose of advising the Government of Canada on threats to the security of Canada, while the RCMP collects evidence that can be used in court proceedings. CSIS can initiate an investigation on the suspicion of conduct that may threaten national security, but the RCMP, as a law enforcement organization, requires a reasonable belief that a crime will be or has been committed. As CSIS obtains more intelligence, it may take increasingly intrusive investigative steps, including applying to the Federal Court for a warrant to intercept a target's telephone or Internet communications. If the behaviour of a subject of investigation reaches a threshold for criminality, CSIS will notify the RCMP, which may initiate a criminal investigation. When the RCMP conducts an investigation, it must be able to disclose information and evidence in court. The RCMP may also seek a court warrant to intercept a suspect's communications or use other intrusive methods of surveillance, such as searches of property or installing tracking devices on vehicles. In some cases, CSIS and the RCMP may conduct parallel investigations to ensure intelligence or evidence is collected to respond to each of their respective mandates. This coordination and cooperation is guided by the terms of the CSIS–RCMP *One Vision* agreement, which ensures the organizations take a collaborative approach to the management of threats.

62. In other cases, the RCMP may investigate a potential threat alone or in coordination with a provincial or municipal police service, or an international partner, such as the United States Federal Bureau of Investigation (FBI). A recent example occurred in August 2016, when the FBI provided the RCMP with information that allowed the RCMP to identify and locate Aaron Driver, a Daesh sympathizer who was planning to attack Union Station in Toronto. The RCMP worked with local police agencies to stop Mr. Driver from conducting the attack, and he was fatally shot in a confrontation with police.

63. Certain security and intelligence organizations can take a number of measures to prevent and disrupt terrorist plots. Police investigations are primarily aimed at laying charges and prosecution. However, not all investigations reach that stage, and police may decide to take other measures to reduce the risks of violent criminal behaviour, such as seeking a peace bond to prevent an individual from engaging in certain behaviours. CSIS and the RCMP may work with Public Safety Canada to place someone's name on the Passenger Protect list. CSIS may also take measures to reduce threats, for example, to make parents aware that their child is accessing extremist material online. For its part, the Canada Border Services Agency (CBSA) may inspect an individual's goods when the individual is seeking entry into Canada, deny non-citizens entry if they are deemed a security risk, and ensure that high-risk individuals are brought to the attention of the appropriate organizations (for example, the RCMP or CSIS).

64. Public Safety Canada plays a leadership and coordination role in fighting terrorism. This department is responsible for Canada's Counter-terrorism Strategy. The Strategy consists of four elements – prevent, detect, deny, and respond – and its overarching goal is to counter domestic and international terrorism to protect Canada, Canadians, and Canadian interests.[11] Public Safety Canada

[11] Public Safety Canada, *Building Resilience Against Terrorism: Canada's Counter-terrorism Strategy*, 2013. Retrieved from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsinc-gnst-trrrsm/rsinc-gnst-trrrsm-eng.pdf.

also plays a leadership and coordination role in countering radicalization to violence, including the establishment of the Canada Centre for Community Engagement and Prevention of Violence.[12]

65. Terrorism investigations are resource-intensive, complex and lengthy. Both CSIS and the RCMP devote considerable resources to investigating terrorist threats. In 2015, the RCMP Commissioner told Parliament that the RCMP had diverted hundreds of federal officers from organized crime investigations to terrorism investigations. The Committee heard that CSIS's and the RCMP's pre-eminent focus on terrorism means that comparatively fewer resources are devoted to other threats, such as organized crime, espionage, or foreign influence activities.

Espionage and foreign influence

66. The second national security threat identified to the Committee by the Privy Council Office was espionage and foreign influence. Espionage activities primarily involve foreign states trying to obtain political, economic, and military information, or proprietary business information, through clandestine means. Foreign influence or interference activities involve foreign states using clandestine or deceptive methods to influence or manipulate Canadian immigrant communities, political parties, and government officials.

67. Russia and China are *** among a handful of states who conduct espionage and foreign influence activities in Canada. Russia has repeatedly sent intelligence agents to Canada to establish false identities and conduct espionage. Examples include a Russian couple known as Ian and Laurie Lambert, whom CSIS discovered conducting espionage activities in 1996 in Toronto and were deported; a Russian man known as Paul William Hampel, who was arrested in Montreal as he tried to leave Canada in 2006; and a Russian couple known as Tracey Foley and Don Heathfield, who had lived in Montreal and Toronto using false Canadian identities and who were arrested in the United States in 2010 and returned to Russia. In January 2012, an officer in the Royal Canadian Navy, Jeffrey Delisle, was arrested for providing information to Russia. He was found guilty and convicted in 2013. In March 2018, Canada expelled four Russian diplomats as part of a coordinated global effort to punish Russia for the poisoning of two people in the United Kingdom, noting that the diplomats had been "identified as intelligence officers or individuals who have used their diplomatic status to undermine Canada's security or interfere in our democracy."[13]

68. China is known globally for its efforts to influence Chinese communities and the politics of other countries.[14] The Chinese government has a number of official organizations that try to influence Chinese

[12] Public Safety Canada, *Canada Centre for Community Engagement and Prevention of Violence*, 2018. Retrieved from: https://www.publicsafety.gc.ca/cnt/bt/cc/index-en.aspx.
[13] Global Affairs Canada, "Canada expels Russian diplomats in solidarity with United Kingdom," Statement by the Minister of Foreign Affairs, March 26, 2018. Retrieved from: https://www.canada.ca/en/global-affairs/news/2018/03/canada-expels-russian-diplomats-in-solidarity-with-united-kingdom.html.
[14] See for example CSIS, "Fingers in all pots: The threat of foreign interference in democratic systems," *China and the age of strategic rivalry: Highlights from an Academic Outreach Workshop*, May 2018; Anne-Marie Brady, *Magic Weapons: China's political influence activities under Xi Jinping*, Wilson Centre, Washington, D.C., September 2017;

communities and politicians to adopt pro-China positions, most prominently the United Front Work Department. The Director of CSIS raised concerns about Chinese influence activities against Canadian politicians in 2010, and a former Canadian Foreign and Defence Policy Advisor to the Prime Minister and later Canadian Ambassador to China stated in 2017 that China used diaspora groups and mobilized Chinese students to influence Canadian politics.[15] In 2016, concerns were raised about wealthy Chinese businessmen with close connections to China's Communist Party making political donations in Canada.[16] Similar issues have been raised in countries with large Chinese diaspora populations. Media and academic reports point to China's efforts in Australia and New Zealand to influence government policies, including through significant political donations, covertly supporting community groups and demonstrations, and influencing Chinese-language media.[17] Chinese police and security officials have also been caught in foreign states operating without permission to persuade or coerce Chinese fugitives to return to China.[18] ***

69. Similar to their roles related to terrorism, CSIS and the RCMP have primary responsibility to investigate and counter espionage and foreign influence. As with other investigations on threats to the security of Canada, CSIS may take a range of measures to investigate and reduce the threat of espionage or foreign influence activities in Canada. The RCMP may conduct a criminal investigation, as it did in the espionage case of Jeffrey Delisle. Global Affairs Canada may be involved should foreign diplomats be found to be conducting such activities and required to leave Canada, as has happened repeatedly with diplomats from Russia and other countries.[19] CSIS officials told the Committee that the threat of espionage and foreign influence was growing in Canada and will likely require a more significant response in the years ahead. The Committee agrees and notes that Australia passed legislation in June 2018 to better prevent, investigate, and disrupt foreign interference.

Cyber threats

70. Cyber threats were another significant national security threat identified to the Committee. In a 2017 study, CSE stated, "nation-states are constantly deploying cyber capabilities to try to gain access to Government of Canada networks and the communications of federal government officials."[20] Russia and

J. Michael Cole, *The Hard Edge of Sharp Power: Understanding China's Influence Operations Abroad*, MacDonald-Laurier Institute, October 2018.

[15] Mike Blanchfield, "Canada should be wary of China's efforts to interfere in its affairs amid pursuit of trade, says former envoy," Canadian Press, December 8, 2017.

[16] Guadalupe Pardo, Robert Fife and Steve Chase, "Trudeau attended cash for access fundraiser with Chinese billionaires," November 22, 2016.

[17] Anne-Marie Brady, *Magic Weapons: China's political influence activities under Xi Jinping*, Wilson Centre, Washington, D.C., September 2017.

[18] Mark Mazzeti and Dan Levin, "Obama Administration Warns Beijing About Covert Agents Operating in U.S.," *New York Times*, August 16, 2015; John Garnaut and Phil Wen, "Chinese police pursued a man to Australia on a 'fox hunt' without permission," *Sydney Morning Herald*, April 15, 2015.

[19] Kathleen Harris, "Canada to expel 4 Russian diplomats, reject credentials of 3 more," CBC News, March 26, 2018. Retrieved from: www.cbc.ca/news/politics/canada-russia-diplomats-sanctions-1.4593062.

[20] Communications Security Establishment, *Cyber Threats to Canada's Democratic Process*, 2017, p. 33. Retrieved from: www.cse-cst.gc.ca/sites/default/files/cse-cyber-threat-assessment-e.pdf.

China are among the most active state actors. Russian cyber threats gained public prominence in the context of the 2016 U.S. presidential election, when Russian intelligence organizations stole data from the campaign of Democratic candidate Hillary Clinton, leaked it through various websites, and used various means, including fake social media accounts, to spread propaganda and disinformation, and to amplify social tensions within the United States. Russian efforts to influence democratic processes in Europe and Africa came to light thereafter. In 2014, a Chinese state-sponsored actor infiltrated the National Research Council of Canada computer networks, causing significant costs for clean-up and remediation. Canada and other countries, including the United States and the United Kingdom, have negotiated agreements with China with the aim of reducing certain Chinese cyber espionage activities.

71. CSE has the primary responsibility for protecting Government of Canada networks from sophisticated cyber intrusions. CSE uses technologically advanced tools to protect government networks from attempts by malicious actors to access and infiltrate those networks. CSE regularly adapts its tools to respond to changes in the technologies and tactics used by those actors, and based on intelligence obtained through its collection efforts and that of its allies. CSE works with Shared Services Canada to secure government networks, and with Public Safety Canada to help protect information systems owned by other levels of government, critical infrastructure providers, and the private sector. On June 12, 2018, the federal government announced a consolidation of government cyber operational units into the Canadian Centre for Cyber Security, led by CSE. This consolidation includes the Canadian Cyber Incident Response Centre, which has operated in Public Safety Canada since February 2005.

Major organized crime

72. Major organized crime was another significant national security threat identified by the Privy Council Office to the Committee. Organized crime has become increasingly sophisticated and global. It is involved in traditional areas of criminality, such as drug trafficking, prostitution, and human smuggling, and more sophisticated forms of 'white collar' crime, such as money laundering, market manipulation, or identity theft. The impact of organized crime is significant and insidious: it undermines public safety, corrupts our legal and political systems, and threatens the integrity of our economy and financial systems.

73. The RCMP's Federal Policing Program employs approximately 5,000 investigators and over 1,000 specialized personnel to conduct investigations across a range of areas. The RCMP is the lead federal organization for investigating and disrupting major organized crime. RCMP investigators use a variety of tools to conduct their work, and may apply to courts for warrants to use the most intrusive techniques, such as intercepting personal communications. The RCMP works with other federal organizations, including CBSA, which is responsible for enforcing legislation related to immigration, customs, and strategic export controls, and the Financial Transactions and Reports Analysis Centre of Canada (more familiarly known as FINTRAC), which is responsible for assessing financial transaction reports and disclosing to the RCMP (and CSIS) financial intelligence that may support investigations of money laundering and terrorist financing. The RCMP also cooperates with Canadian police services and international partners, especially through the Five Eyes Law Enforcement Group and Interpol, to investigate crimes with an international dimension.

Weapons of mass destruction

74. The proliferation and potential use of weapons of mass destruction was another national security threat identified to the Committee. These weapons include nuclear, chemical, radiological, or biological weapons that could cause widespread and indiscriminate destruction. [*** This text cites an assessment and names a country that poses an increasing threat.***] The community is also concerned about foreign states trying to obtain civilian technologies – such as software used to encrypt telecommunications or sophisticated laser equipment ("dual use" technologies) and delivery systems subject to control lists or sanctions – that could be used to develop military technologies to threaten Canada and its allies.

75. The security and intelligence community works together to address the proliferation threat. For example, Global Affairs Canada is responsible for the administration of a number of laws designed to prevent the proliferation of weapons of mass destruction or the export of dual use technologies. Innovation, Science and Economic Development Canada is responsible for reviews of investments that may be injurious to national security under the *Investment Canada Act*. In each case, departments rely on the expertise and intelligence of organizations such as CSIS, CSE, DND, the RCMP, and Public Safety Canada to provide advice to ministers or to make decisions on specific export applications. The RCMP may also conduct investigations of individuals or companies suspected of violating Canadian laws in this area.

Promoting Canadian interests

76. Aside from addressing security threats, intelligence is used to advance Canadian interests in the areas of international relations, national defence, and national security. Canada is an active player on the world stage. It devotes considerable attention to building and maintaining bilateral relations with countries in key regions. It plays important roles in many multilateral organizations that focus on issues like trade and security. It deploys personnel around the world in support of Canadian foreign policy and security priorities, including peacekeeping and military missions, humanitarian and aid projects, or crisis situations that require support for Canadians abroad. In each of these circumstances, the government and its officials use intelligence to improve its understanding of a situation, develop the most appropriate or advantageous policies, and maximize the effectiveness of its operations.

77. A number of organizations collect and assess intelligence in support of these interests. CSE collects foreign intelligence in accordance with the government's foreign intelligence priorities. CSIS may collect intelligence within Canada relating to Canada's defence or international affairs at the request of the Minister of National Defence or the Minister of Foreign Affairs. It may also report intelligence that it obtains in the course of a security investigation. CSE and CSIS intelligence reports are produced by personnel in each organization and provided on a need-to-know basis to specially cleared officials in over 20 government departments and relevant ministers through a highly classified communications network or through Client Relations Officers. Global Affairs Canada obtains privileged information through its personnel posted abroad and distributes its reports through a classified network. For its part, DND/CAF uses its intelligence capabilities to support forces deployed abroad (this will be discussed in greater detail in chapter 4).

78. A number of organizations write intelligence assessments for the use of a broad range of officials, including senior government officials and ministers. An assessment usually involves multiple sources of information or intelligence, including media reports, academic research, privileged contacts, metadata, or highly classified information from human sources or intercepted communications. Assessments may be used by policymakers and operational departments as contextual information, to support policy deliberations, or to refine or change operational programs. Strategic assessments of major international issues are developed by the Privy Council Office Intelligence Assessment Secretariat. Assessments of the threat posed by terrorism to Canada are done by the Integrated Terrorism Assessment Centre. CSIS develops and distributes assessments on security threats to Canada. CSE conducts assessments on cyber threats and cyber security, as they relate to federal government systems and information infrastructures of importance to the Government of Canada. Global Affairs Canada conducts assessments on threats to diplomatic missions. DND/CAF conducts a range of assessments on military issues, from tactical (to support deployed operations) to strategic (to support decision-making on military deployments).

Conclusion

79. Numerous departments and agencies comprise Canada's security and intelligence community. These organizations have diverse mandates and responsibilities, but work together to keep Canadians safe and to promote Canadian interests. The governance and cooperation of these organizations are managed through a number of specific committees that meet regularly to discuss operational and policy issues of common concern. Those organizations also cooperate and share information to varying degrees among themselves, depending on where their specific operational authorities and mandates may intersect. The following two chapters will review how the Government of Canada identifies and implements intelligence priorities, an important mechanism for the governance and accountability of Canada's security and intelligence community, and will review intelligence activities and authorities of DND/CAF, one of the security and intelligence community's core members. The Committee hopes that, together, this information will not only help to improve the effectiveness and accountability of Canada's security and intelligence community, but will also help Canadians better understand how the community functions and the specific activities of some of its key members.

Chapter 3: Review of the Process for Setting Intelligence Priorities

Introduction

80. As one of its first reviews, the Committee examined how the Government of Canada sets intelligence priorities. This review – the first since the Office of the Auditor General examined it in 1996 - provided the Committee with a broad view of the framework for how Cabinet and the various government departments and agencies involved in intelligence set and respond to priorities, requirements, and demands. This review is foundational. The Committee is new and has a mandate to review the framework of national security and intelligence in Canada. Future reviews will build on this one, as the Committee examines other parts of the framework to help support and maintain an effective, responsive, responsible, and accountable national security and intelligence community.

81. The Committee believes that it is uniquely placed to examine this issue. NSICOP is the first external and independent review body able to comprehensively examine national security and intelligence from a strategic perspective and across organizations, and with access to classified information. This allows it to review the process by which the security and intelligence community receives and responds to direction.

82. The importance of the process for setting intelligence priorities cannot be overstated. In Canada, Parliament serves as the highest form of democratic accountability. Ministers are accountable to Parliament and to Canadians for the activities and conduct of the departments and agencies in their portfolios. Within Cabinet, ministers are accountable to the Prime Minister. For most areas of public policy, this system encourages discussion and debate and is the foundation of ministerial accountability.

83. In the area of intelligence, ensuring accountability is a challenge. Intelligence is almost always classified to protect sources, methods, and access to targets, meaning that ministers and officials from organizations that collect or use intelligence cannot be **publicly** held to account the way that other officials can. Nor can they be as transparent about their activities and decisions. Intelligence activities have the potential to impact the rights of Canadians through, for example, intrusive investigative methods. Intelligence activities are also increasingly integrated, meaning that more than one minister is responsible for the overlapping activities of the security and intelligence community, which makes coordination particularly important.

84. Because of the sensitivity of targets, sources, and methods, the potential impact of intelligence activities on the rights of Canadians, and the possibility of gaps, intelligence activities carry an inherent amount of risk. For example, the disclosure of an intelligence target, such as a foreign state, could cause significant damage to Canada's foreign relations; the disclosure of a source identity could put an individual at significant risk. Another component of risk is "opportunity cost" – not all issues can be covered by a security and intelligence community of limited size and scope. Decisions must be made about where to focus and where not to focus, including by Cabinet at the strategic level.

85. Over time, the government has put in place measures to ensure the accountability of the security and intelligence community. These include legislation that defines the authorities and limitations of

security and intelligence organizations, court warrants, and specialized review bodies. From a process perspective, the most important measure is the setting of intelligence priorities. It is the primary mechanism through which the government provides direction to the security and intelligence community and holds it accountable. In short, the intelligence priorities process is a vital part of ensuring accountability and managing risk.

86. The Committee examined the process for setting intelligence priorities from three angles. These were the governance of the process, the participation of the organizations involved, and performance measurement and resource expenditures. The Committee received significant information from all departments and agencies involved in the process.[1] It conducted hearings with the Security and Intelligence Secretariat of the Privy Council Office (PCO), Public Safety Canada, CSIS, CSE, Global Affairs Canada, PCO's Intelligence Assessment Secretariat, the Integrated Terrorism Assessment Centre, and Immigration, Refugees and Citizenship Canada. These organizations are representative of the key intelligence collectors and those with important coordination roles, intelligence clients with extensive requirements and those with program-specific requirements, and intelligence assessment organizations. The departments and agencies involved cooperated well with the Committee throughout the review process.

87. Overall, the Committee believes that the process for setting intelligence priorities has a solid foundation and has improved over time. Cabinet provides regular direction to the security and intelligence community. That direction is filtered through interdepartmental mechanisms into specific requirements that help guide the work of intelligence collectors and assessors. The process is governed by a defined committee structure and a performance measurement framework, which supports regular updates to ministers and Cabinet. However, every process can be improved and the security and intelligence community recognizes this. The Committee's review revealed challenges in a number of areas, some of which have already been identified by organizations within the security and intelligence community. These areas include inconsistencies in ministerial direction and the operational implementation of priorities, ensuring that Cabinet has sufficient information to support its discussions and decision-making, underdeveloped performance and financial reporting, and insufficient central leadership. The Committee believes that, together, these challenges can undermine ministerial accountability for intelligence activities.

88. These challenges should be addressed. As described earlier, accountability is a fundamental condition for the proper conduct of intelligence activities. Indeed, the Committee notes that accountability, and intelligence priorities by extension, have been a core feature of two external reviews of intelligence since the 1980s – one by an Independent Advisory Team and the other by the Office of the Auditor General. Accountability must be constantly renewed to be meaningful. The Committee therefore makes recommendations that it believes will strengthen the accountability, efficiency, and effectiveness of the security and intelligence community.

[1] CSIS, CSE, DND, RCMP, Canada Border Services Agency, Financial Transactions and Reports Analysis Centre, PCO, Public Safety, the Integrated Terrorism Assessment Centre, Global Affairs Canada, Transport Canada, and Immigration, Refugees and Citizenship Canada.

89. The Committee's review was itself not without challenges. One of the biggest was that NSICOP is legislatively prohibited from seeing "Confidences of the Queen's Privy Council." These confidences are defined in the *Canada Evidence Act*, and include any information used to present proposals or recommendations to Cabinet; used as analysis or background for consideration by Cabinet in making decisions; contained in records of deliberations for decisions of Cabinet; contained in records used for communication or discussions between ministers; contained in records to brief ministers in relation to matters that are before, or will be before, Cabinet; or contained in draft legislation.[2] Given that the process for setting intelligence priorities involves memorandums to Cabinet and records of decision, that restriction made it difficult for the Committee to examine and consider all of the relevant information on this topic. This review and the Committee's findings and recommendations are therefore based on documentation and information, including drafts, created through the intelligence priorities setting process up to the deputy minister level. The Committee believes it was sufficiently informed to make its findings and recommendations.

[2] *Canada Evidence Act*, (R.S.C., 1985, C.5 C-5), subsection 39(2). Retrieved from: http://laws-lois.justice.gc.ca/eng/acts/C-5/

A short history of Canada's intelligence priorities

90. The process for setting intelligence priorities is described by PCO as "the primary mechanism available to the Prime Minister, Cabinet and senior security and intelligence officials for exercise and control, accountability and oversight of Canada's intelligence production."[3]

91. The process has evolved over time. Cabinet first set national intelligence priorities in the 1970s, but these were narrowly defined and focused on foreign intelligence. In 1987, an Independent Advisory Team led by the Honourable Gordon Osbaldeston examined the newly created CSIS. The report, *People and Process in Transition*, made several recommendations, including that "the primacy of the role of the political executive in the provision of direction in the national security framework must be re-emphasized," and that CSIS should seek Cabinet approval for its priorities on an annual basis.[4] Since then, CSIS has sought approval for its security intelligence priorities.

92. Throughout the 1990s, the process of setting Government of Canada intelligence priorities expanded beyond a relatively narrow focus to include other areas, such as defence. The priorities became increasingly detailed and categorized along departmental lines. In 1996, the Office of the Auditor General conducted a review of the accountability of the security and intelligence community in Canada. It recommended "enhancing the national priorities process through clearer tasking against priorities, more timely approvals, a more complete ranking system and systematic assessment of intelligence collection against approved priorities." The community responded by stating that the recommendations coincided with its objectives and that "the development of clear priorities to guide intelligence collection and reporting efforts is more important than ever, given that the Canadian intelligence community has more consumers interested in more topics, while, at the same time, it has fewer resources to do the job."[5]

93. The process continued to evolve in response to new priorities and government direction. After the terrorist attacks of September 11, 2001 in the United States, the Government increased the number of priorities and realigned their importance, but made no major changes to the overall process. In 2006, the Government approved a proposal to refocus the process on a smaller number of ranked strategic themes. These broad themes allowed the priorities to better fit within the mandates of all organizations involved in intelligence in Canada.

94. In 2016, the Government decided not to rank the intelligence priorities in the same way that it had for the previous 10 years. PCO informed the Committee that this was due to a number of factors. Following the 2014–2016 priorities-setting cycle, PCO assessed the security and intelligence community's spending, intelligence production, and requests for collection requirements. It found that, in general, spending levels, intelligence production, and requests for intelligence collection did not align

[3] Privy Council Office, Intelligence Priorities Binder Overview for the NSIA, April 2015.
[4] Independent Advisory Team, *People and Process in Transition*, Report to the Solicitor General on the Canadian Security Intelligence Service, October 1987.
[5] Office of the Auditor General of Canada," The Canadian Intelligence Community– Control and Accountability," Chapter 27 in *Report of the Auditor General of Canada – 1996*, November 1996.

with the ranking of the intelligence priorities. In other words, departments and agencies spend more and have more requests for collection on some lower-level priorities than higher-level priorities. The only exception was the *** priority, where the priority level of those issues and the community's level of effort against them were generally consistent. In addition, PCO noted that many departments that receive intelligence for the purposes of their work, but do not collect it, expressed frustration that their needs for intelligence ranked too low to merit sufficient attention by the organizations responsible for intelligence collection. Other organizations believed that the ranked priorities could be perceived as inconsistent with their different mandates. Moreover, PCO noted that ***. PCO noted that by eliminating the ranking of priorities and addressing the issue at the more detailed level of intelligence requirements (further described below), the security and intelligence community could better respond to these challenges. The intelligence priorities for 2017-2019 are listed on page 38.

What is the process for setting intelligence priorities?

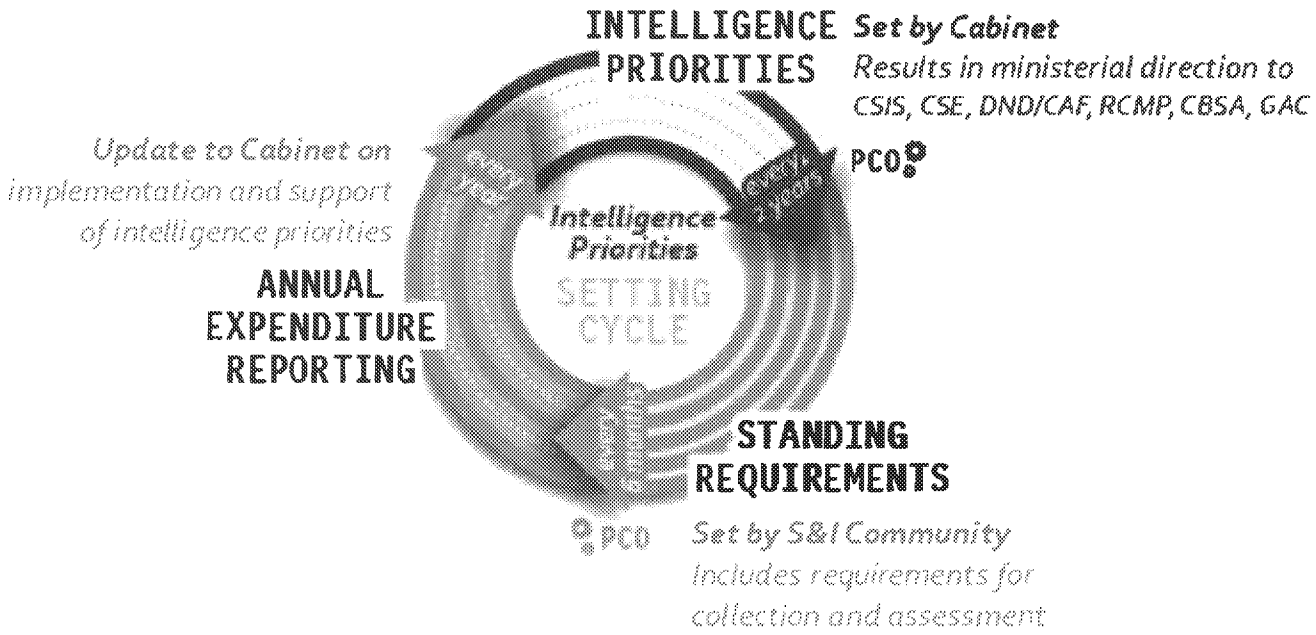
95. For the period reviewed by the Committee, Government of Canada intelligence priorities were set by the Cabinet Committee on Intelligence and Emergency Management.[6] This Cabinet committee's role was to consider reports and priorities, and to coordinate and manage responses to public emergencies and national security incidents. It was chaired by the Prime Minister, reflecting his or her overarching responsibility for intelligence and national security. The Committee included ministers with responsibility for key organizations that work in the areas of security and intelligence, specifically the ministers of Public Safety and Emergency Preparedness, National Defence, and Global Affairs. The process to set intelligence priorities is depicted on page 38.

[6] On August 28, 2018, the Government announced changes to its Cabinet committees. The Cabinet committee that now establishes the intelligence priorities is the Cabinet Committee on Canada, the World and Public Security.

Intelligence Priorities for 2017-2019

Intelligence priorities are broad areas of focus set by Cabinet based on where government departments require information to make decisions or fulfill their mandates. The current intelligence priorities are:

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



96. The current procedure is for the security and intelligence community to seek Cabinet approval on the intelligence priorities every two years. First, participating ministers are presented with a memorandum to Cabinet drafted by PCO's Security and Intelligence Secretariat. Cabinet decides on the strategic priorities, and a Record of Decision is issued, as per standard Cabinet process. Drawing from this Record of Decision, the Ministers of Public Safety and Emergency Preparedness, National Defence, and Foreign Affairs, as the ministers responsible for the largest collectors of intelligence, issue direction to their respective organization(s) articulating the priorities and the minister's expectations.

97. The departments and agencies then use those intelligence priorities and the direction they have received from their minister to create the interdepartmental Standing Intelligence Requirements (SIRs), a breakdown of more detailed collection and assessment requirements. The SIRs are reviewed and updated at least every six months. In that process, organizations that collect, assess, and use intelligence articulate their capabilities to respond to the requirements and detail their own intelligence needs. The requirements are updated as necessary based on emerging issues. The ongoing engagement of the security and intelligence community on the SIRs, coordinated by the Security and Intelligence Secretariat, assists in making collection and assessment more responsive to a fluid foreign, security, and defence environment. These processes are coordinated and managed by the Security and Intelligence Secretariat and overseen by the Prime Minister's National Security and Intelligence Advisor (NSIA).

98. Finally, PCO updates the Cabinet committee annually on how the community has supported the intelligence priorities by detailing the implementation and support by each organization. This is done in part through the National Intelligence Expenditure Report, which is managed by Public Safety Canada and coordinated by the Security and Intelligence Secretariat of PCO. This expenditure report includes resource expenditures by intelligence priority and by function (such as collection, production, or support) and is designed to demonstrate to Cabinet the extent to which intelligence production and resource allocation supports the priorities.

99. For many years, the priorities process focused almost exclusively on intelligence collection. In 2013, the Intelligence Assessment Secretariat of PCO and the Integrated Terrorism Assessment Centre were brought into the process. The security and intelligence community noted that this change:

- led to better representation of intelligence organizations with responsibilities for collection, assessment, or both;
- provided the assessment community with strengthened guidance and direction to facilitate prioritization of assessment production;
- led to closer collaboration between assessment organizations and their security and intelligence partners; and
- brought a wider spectrum of intelligence – collection and assessment – under the intelligence priorities governance and accountability framework.

The result is that government direction on intelligence now includes all relevant organizations.

Governance

100. The intelligence priorities are intentionally broad. They are designed to capture the government's strategic policy and operational requirements and be relevant to the various mandates of the departments and agencies involved in intelligence. Those organizations include:

- the two largest intelligence organizations, CSIS and CSE;
- departments involved in intelligence, either as collectors or assessors or both, such as the Department of National Defence/Canadian Armed Forces (DND/CAF), Global Affairs Canada, the Integrated Terrorism Assessment Centre, and the Royal Canadian Mounted Police (RCMP); and
- organizations that are significant clients of intelligence but with a primary role outside of intelligence, such as Transport Canada and Immigration, Refugees and Citizenship Canada.

101. The security and intelligence community is involved in this process at multiple levels. PCO, in the form of the NSIA and the Security and Intelligence Secretariat, leads and coordinates the process. The Secretariat writes the Memorandum to Cabinet in coordination with the security and intelligence community, and leads the interdepartmental process to develop the detailed SIRs. At the deputy minister level, the NSIA co-chairs the Deputy Minister National Security Committee, the primary committee at the deputy minister level for strategic conversations about intelligence and national security. This committee considers the draft memorandum and recommends that it be provided to Cabinet. Those deputy ministers are responsible for ensuring departments are responding to and compliant with ministerial direction.[7]

102. At the Assistant Deputy Minister (ADM) level, the Security and Intelligence Secretariat chairs the ADM Intelligence Committee that approves and attests to the requirements, performance measurement, and resource allocation. At the working level, the Security and Intelligence Secretariat leads several working groups that hold detailed negotiations and discussions on the prioritization of specific requirements. These committees and working groups help to support Cabinet in setting and responding to the intelligence priorities. The Security and Intelligence Secretariat's role in this process is fulfilled with minimal resources. In a briefing note to the Assistant Secretary for Security and Intelligence, officials noted that there was " *** devoted to supporting the intelligence coordination activities" and that "with current resource levels, we have not been able to maintain consistent levels of coordination with the intelligence community."[8]

103. PCO is ideally placed to provide governance and leadership on intelligence priorities. Under the NSIA, the Security and Intelligence Secretariat directly supports the Cabinet committee responsible for considering the intelligence priorities. Its role is to advise Cabinet on security and intelligence issues from the broadest governmental lens, and is therefore well placed to play a leadership, coordination,

[7] Privy Council Office, Security and Intelligence Secretariat, Assistant Secretary to Cabinet, NSICOP Hearing, June 14, 2018.
[8] Privy Council Office, Security and Intelligence Secretariat, "Intelligence Coordination Pressures," Memorandum for the Assistant Secretary to Cabinet, November 8, 2016.

and mediation role in the development of the Memorandum to Cabinet and through its supporting processes. This model has been noted by allies with similar governmental structures. In Australia, the 2017 Independent Intelligence Review recommended that the Australian government centrally coordinate its intelligence as its allies, including Canada, have done. The report stated that more effective coordination would "enhance . . . Ministerial responsibility and the intelligence community's accountability to the Government" and that "enterprise-level management . . . will complement the statutory responsibilities of agencies."[9] While Canada's system has a structure in place to provide coordination and management, investment and focus have been lacking. For this system to be optimal, strong and sustained central leadership and governance are necessary.

Ministerial Direction

104. Following Cabinet's approval of the intelligence priorities, the ministers responsible for each of the primary organizations involved provide written direction articulating their expectations for how each organization will respond to the priorities. Which organizations receive ministerial direction has changed over time. In the past, direction was generally provided only to the core departments and agencies involved in the collection of intelligence – CSIS, CSE, the RCMP, DND/CAF and Global Affairs Canada. Beginning with the 2017–2019 intelligence priorities, the Canada Border Services Agency (CBSA) also received Ministerial Direction on implementing those priorities. Ministerial direction for enforcement organizations, the RCMP and CBSA, is drafted to preserve their operational independence.

105. Ministerial direction tailors the intelligence priorities to the specific legal mandates and operational responsibilities of the organizations. For example, direction to CSIS would highlight the priorities directly related to the CSIS mandate, such as [*** name of priority ***]; direction to the RCMP would highlight [*** name of priority ***].

106. In the current system, once the Cabinet record of decision is issued, each organization writes its own direction for its minister's approval. This causes some important inconsistencies. In some cases, departments or agencies were not timely in drafting the direction.[10] Delays in providing ministerial direction may affect the responsiveness of government organizations to new direction and the timing of intelligence collection. Delays may affect the accuracy and scope of performance reporting back to Cabinet, particularly when priorities change. Delays may also put organizations and their management at risk.[11] Ministerial directions exist in part so that when a department or agency undertakes national security or intelligence activities, the minister can be accountable for those activities. If they are issued late and a problem arises, the minister may not be able to confirm that she or he was aware of what the organization was doing.

107. The Committee discusses these latter two issues in more detail later in this chapter. The Committee also notes that some ministerial direction contained inconsistencies in wording or

[9] Commonwealth of Australia, 2017 Independent Intelligence Review, 2017.
[10] Privy Council Office, Implementing the 2017–2019 National Intelligence Priorities – Privy Council Office Role and Deliverables, November 8, 2016.
[11] PCO Response to NSICOP Review of the National Intelligence Priorities, October 2018.

expectations, which may affect subsequent performance reporting to Cabinet. For example, in 2017–2019, the Ministerial Direction drafted by CSIS excluded two of the priorities, [*** names of priorities ***], and the [*** names of priorities ***].[12] Of note, the omission of [*** name of priority ***] created confusion within CSIS over whether its officers could collect intelligence on an issue that was an intelligence priority, had been identified as a very high priority of the community in the SIRs, and was within the mandate of CSIS to collect.[13] These inconsistencies undermine the effectiveness and efficiency of the community and the Minister's accountability.

108. Led by PCO, the community is taking specific measures to address issues related to consistency and timing of the Ministerial Directions associated with the intelligence priorities. These measures also aim to enhance the role of the NSIA in monitoring performance with respect to this aspect of the process.[14]

[12] Ministerial Direction to CSIS on the Intelligence Priorities, 2017–2019.
[13] Emails between CSIS and PCO / Security and Intelligence Secretariat, June 19, 2018; Client Questionnaire – ***, CSIS Response, September 2014; and Standing Intelligence Requirements Client Questionnaire – Feedback on *** Intelligence Support, CSIS Response, April 2015.
[14] Scenario Note, Meeting of the ADM Intelligence Committee, January 23, 2018.

Standing Intelligence Requirements

109. The SIRs are a list of specific requests from clients for collection or assessment based on the intelligence priorities. Simply put, the SIRs reflect the intelligence that departments need to do their jobs. Currently, there are over 400 Requirements. The SIRs are ranked into four tiers by importance and the risk or threat that they pose, based on criteria approved by the Government in 2016. Updated every six months and on an ad hoc basis when issues emerge, they are negotiated at the working level and approved by the ADM Intelligence Committee.

Standing Intelligence Requirements

SIRs are far more detailed items that fall under each of the intelligence priorities. They drive the collection of intelligence and the development of assessments. For example, under the *** priority, a SIR might be information on a specific *** group, such as ***.

110. The SIRs seek to provide an overall picture of what the community is collecting and assessing, where there are gaps, and in what areas the community remains dependent on reporting from allies, such as the Five Eyes. ***. The SIRs can also provide details on how much individual organizations, and the security and intelligence community as a whole, can address (i.e., collect on or assess) any priority or requirement. This type of information is vital for accountability: to provide informed direction, ministers need to have enough information to understand the implications of their decisions.

111. The Committee is concerned that Cabinet may not have access to information that would inform its decision-making. In 2016, PCO introduced a new framework to improve the process for prioritizing the many specific demands of the community within the SIRs. In 2017, the community also considered a new approach that would provide more detailed reporting to Cabinet, including:

- an estimate of the capacity and intention of each organization to either collect on or assess the SIRs;
- which priorities generate the most demand for collection through the SIRs process; and
- the top intelligence targets of the community as a whole.

112. This option would have shown that the community had the capacity and intention to collect on *** percent of SIRs identified at the highest level of importance and on *** percent on the SIRs overall. A PCO document drafted in preparation for the ADM Intelligence Committee noted that the approach was, "an opportunity to use useful data that is generated through the requirements process to support strategic-level discussion on intelligence coordination."[15] However, a much later draft considered by the community did not contain the detail listed above. Instead, the draft provided a chart showing, in order,

[15] Assistant Deputy Ministers Intelligence Committee, Discussion on priorities-related data, Committee meetings, October 2017 and November 2017.

the intelligence priorities by "level of intelligence effort,"[16] but without quantified data. The Committee does not know whether the more informative data generated by the interdepartmental working group was ultimately provided to Cabinet, but it does believe that specific data would provide ministers with valuable context. PCO informed the Committee that it is considering options for making better use of the information generated through the SIRs to develop more strategic assessments on intelligence demand and support.[17]

113. The Committee discussed the processes for setting the intelligence priorities and the SIRs with several organizations at hearings. Two themes emerged: the challenge inherent in the level of detail of the SIRs, and the constant pressure to add more to the list. CSE noted to the Committee that the community has many tactical conversations around the SIRs, but that there is room for more strategic discussion around the SIRs and their context within the process to set the intelligence priorities.[18] The Committee agrees that such an overview would be of benefit to Cabinet. A full picture of government capacity to address the SIRs and the priorities from which they derive, including where compromises have been made, would enable Cabinet and ministers to make informed decisions about trade-offs and risk management. Without those strategic considerations, the demands for intelligence become increasingly unmanageable.

114. The Committee is concerned that the security and intelligence community may be reaching that point. Demands for intelligence that have been identified in the interdepartmental process have resulted in a great many SIRs: currently there are over 400 separate requirements. At hearings, the Committee heard a consistent message from all departments and agencies involved in this process: there are too many SIRs, making the process "cumbersome" and less responsive than most participating organizations would like. For its part, Global Affairs Canada, the largest client organization, informed the Committee that it must be more rigorous in its own internal prioritization to decrease the number of demands it is making for collection and assessment and to enhance focus.[19] PCO also noted that the community needs to develop tools to manage these challenges strategically.[20] The Committee is aware that PCO has made other efforts in the last several years to streamline the process. With *** percent of SIRs being covered, and *** percent of the highest priority requirements, the Committee believes there is still room for improvement.

115. The Committee is similarly concerned about the completeness of information being provided to Cabinet in other areas. Consistent with subsection 14(*a*) of the *NSICOP Act*, the Committee was not able to review the Memorandums to Cabinet on the intelligence priorities: those memorandums constitute a confidence of the Queen's Privy Council, one of four exceptions to the information that NSICOP is entitled to have. Nonetheless, based on information that was provided about the process of developing that advice, the community appears to provide Cabinet primarily with information and anecdotes that

[16] Draft CCIEM Update on Intelligence Priorities Implementation V.31., Memorandum for NSIA, Fall 2017 Update on Intelligence Priorities Implementation to Cabinet Committee on Intelligence and Emergency Management. November 28, 2017.
[17] PCO Response to NSICOP Review of the National Intelligence Priorities, October 2018.
[18] Director General of Intelligence Operations, CSE. Follow up to NSICOP Hearing. June 25, 2018.
[19] Deputy Minister, Global Affairs Canada, NSICOP hearing, June 14, 2018.
[20] PCO Response to NSICOP Review of the National Intelligence Priorities, October 2018.

highlight where the community has had operational successes and where it has responded to government direction.[21]

116. The community has been less effective at highlighting gaps in collection and analysis, and the trade-offs and risk management associated with collecting intelligence in some areas and not in others (as described earlier, the opportunity cost inherent in prioritization). In one example of an opportunity cost, the Security and Intelligence Secretariat informed the NSIA that some organizations "have noted that relatively large expenditures on [*** name of priority ***] have continued to increase while pressures related to [*** name of priorities ***] have also grown," but that that information would not be part of the information update to Cabinet.[22] The Committee recognizes that compromises around intelligence collection and assessment priorities must be made given the relatively small size of Canada's security and intelligence community. For that reason, the Committee believes it is important to ministerial accountability that those compromises be explained to the Cabinet committee and that the implicated ministers receive the information required to properly assess the decisions before them, including to evaluate the risks inherent in prioritization.

117. Ultimately, the process for setting intelligence priorities is important to the functioning, management, and accountability of the security and intelligence community. It provides a forum for discussion and debate, as well as compromise and coordination. However, the process itself is only as strong as the sum of its parts. The goal, which is robust accountability, requires sound management and a consistent and coordinated framework. Ministerial accountability and the effectiveness and efficiency of the community are best served by ensuring that Cabinet has the most complete information at its disposal. As will be discussed later, the decision to use simplified reporting on results, and the lack of consistent investment in the process to further develop reporting tools, has weakened the process. Those decisions have also contributed to inconsistencies by some organizations in this process. The Committee turns to this issue next.

[21] Privy Council Office, Draft Summary of Highlights, December 11, 2017.
[22] Privy Council Office, Security and Intelligence Secretariat, "Fall 2017 Update on Intelligence Priorities Implementation," Memorandum to NSIA, November 28, 2017.

Operationalization

118. The Committee reviewed how the individual departments and agencies involved in this process operationalize the intelligence priorities and the SIRs, that is, how they take the priorities and develop specific collection plans. Most departments and agencies have created methods for articulating the priorities and requirements into specific direction and guidance for their own activities. The three largest – CSIS, CSE, and DND/CAF – have formalized processes. These processes further refine the SIRs in the context of the mandate, capabilities, and direction of each organization.

119. Each organization uses similar methodologies to develop internal priorities. Each uses weighted methods (assigning a point value to an issue based on its importance to the community, the tiering of the SIRs, the direction of the minister, the relevance to its mandate, and the organization's capacity and ability to collect) to develop internal documents that provide working-level collectors with detailed direction that guides collection and tracks performance. These documents are CSIS's Intelligence Requirements Document, CSE's National SIGINT Priorities List,[23] and DND/CAF's Strategic Defence Intelligence Requirements.

120. This tailoring of the SIRs is important to ensure that priorities and requirements align with the individual mandates of the specific organizations responsible for intelligence collection and assessment, and to provide sufficiently detailed direction to officials responsible for the organization's intelligence activities.

121. The processes for setting intelligence priorities and establishing the SIRs allow for variance in how much is required of an organization based on its role in the security and intelligence community. The highest expectations for participation and reporting are on the two primary collectors of intelligence: CSE and CSIS. Those two organizations have in the past few years adopted significantly different approaches to meeting those expectations.

The Communications Security Establishment

122. CSE is Canada's signals intelligence agency. It is the only organization with a statutory requirement – that is, required by law – to provide intelligence in accordance with the intelligence priorities.[24] As a result, CSE is heavily invested in the process to set intelligence priorities. This investment has resulted in a rigorous, consistent, and timely internal process to support the overall intelligence priorities. CSE uses the intelligence priorities and the SIRs to develop internal collection priorities that allow it to respond to government and client priorities and needs. CSE reports the results of its performance and expenditures to its minister through an annual report and to Cabinet through the intelligence priorities process (that is, through the interdepartmental Memorandums to Cabinet and related updates). In addition, CSE has made strategic decisions regarding its resource allocation based

[23] SIGINT stands for signals intelligence, but for CSE it refers specifically to foreign signals intelligence. The "National" in the title refers to the priorities, not to the type of signals intelligence.
[24] *National Defence Act*, 1985, paragraph 273.64(1)(*a*).

on the priorities and the SIRs, expending approximately *** percent of its resources on the highest priority requirements.[25]

The Canadian Security Intelligence Service

123. CSIS also has an internal process to translate the broader priorities and requirements into collection priorities that are used to drive its operations, reporting, and assessment. Like CSE, this is a longstanding process that also allows CSIS to track its collection and production for reporting purposes. That internal direction is updated every six months following the updating of the SIRs. However, CSIS senior management approved the internal direction (a necessary step) in September 2016 and then not again until April 2018, resulting in an implementation gap that exceeded a year.[26] CSIS officials informed the Committee that this lapse in implementing the internal requirements had no material impact on CSIS collection activities because there were no fundamental or significant differences between the previous priorities and requirements and the new ones. CSIS stated that it continued to collect intelligence on threats to the security of Canada and maintained that it was always compliant with Ministerial Direction.[27]

124. In the Committee's view, this delay by CSIS affected the entire security and intelligence community. The reliance on outdated or inaccurate internal requirements will make it difficult to fully account for CSIS activities and to provide the most complete information to Cabinet on how the intelligence priorities were supported. Also, CSIS will not be able to provide reliable production measures on the SIRs. This will mean that the security and intelligence community will face challenges in evaluating its overall coverage of the SIRs and the intelligence priorities. The Committee believes that this lapse weakened the accountability that the system was intended to provide.

125. Finally, there is the example this sets for the community. As the Committee noted in its introduction, the intelligence priorities setting process has improved over the years – an acknowledgement made by every department and agency involved. This process, however, is only as strong as the sum of its parts. CSIS and CSE are the most important intelligence collection organizations in the government. As such, the Committee expects that CSIS would take a leadership role in developing and implementing the intelligence priorities and the SIRs and measuring its ability to respond to them.

126. As a result of this review, CSIS noted to the Committee that it has initiated new oversight structures and several improvements to the way it directs and prioritizes collection efforts to better

[25] CSE, Director General Intelligence Operations, NSICOP hearing, June 21, 2018.
[26] Deputy Ministers Intelligence Assessment Committee, Discussion on Update on Intelligence Priorities Implementation – Scenario Note, November 28, 2017; Assistant Deputy Ministers Intelligence Committee, Scenario Note, October 24, 2017; CSIS, Assistant Director Intelligence, NSICOP hearing, June 21, 2018; and NSICOP draft report of Review of Intelligence Priorities – CSIS Views, Corrections and Clarifications. August 27, 2018.
[27] CSIS, Assistant Director Intelligence, NSICOP Hearing June 21, 2018; CSIS, Deputy Director General, Intelligence Assessment Branch, May 23, 2018; CSIS, Director General, Intelligence Assessment Branch, and CSIS Deputy Director General, Intelligence Assessment Branch, CSIS, July 13, 2018; 2016-2017 Intelligence Requirements Document (IRD), 2nd Edition, September 15, 2016; 2018–2019 Intelligence Requirements Document (IRD) – 1st Edition, April 4, 2018; and CSIS comments to NSICOP on draft report, October 2018.

understand client needs. It is also undergoing a review of its intelligence requirements system to assess the manner in which it translates the intelligence priorities into requirements and direction for its collection activities. CSIS is working with PCO to support ongoing improvements to the SIR process.[28]

Assessment organizations

127. The intelligence priorities process has become more inclusive with the formal addition, in 2013, of the Intelligence Assessment Secretariat of PCO and the Integrated Terrorism Assessment Centre. By bringing these assessment organizations closer in line with government priorities and the requirements of the community, client organizations (i.e., those departments and agencies that obtain intelligence and assessments to support their legal mandates) stated that they receive more relevant analysis and more informative products on their areas of operation.[29] Departments and agencies noted that the assessment of intelligence provides context and perspective on the intelligence available to the community, and stated that the inclusion of the assessment organizations in the intelligence priorities process had been of benefit to the process and the security and intelligence community. This inclusion also provided an opportunity for the Integrated Terrorism Assessment Centre to communicate directly its requirements and preferences with respect to intelligence requirements and priorities independent of others in the community, including CSIS, on whose premises it is co-located.

128. In addition, the Committee was informed that the inclusion of intelligence assessment as part of the intelligence priorities process has started to reach beyond stand-alone assessment organizations. For the first time, CSIS shared its assessment production plan with the working group for the SIRs and the ADM Intelligence Committee. CSIS shared this information in "an effort to be more transparent, enabling better de-confliction and coordination within the [security and intelligence] analytic community."[30] The Committee sees these trends as positive developments.

[28] Canadian Security Intelligence Service, Response to NSICOP Review of the National Intelligence Priorities, November 2018.
[29] Immigration, Refugees and Citizenship Canada, Associate Assistant Deputy Minister of Strategic and Program Policy Sector, NSICOP hearing, June 14, 2018.
[30] CSIS, Email from Director General Intelligence Assessment Branch, March 7, 2018.

Resource expenditures and performance measurement

129. Another aspect of accountability is measuring performance and expenditures against priorities. Over the last decade, successive governments have emphasized the value of measuring the performance of government operations and have implemented new means of tracking organizational performance and accounting for related expenditures. These are important means of ensuring control and accountability. The importance of assessing the effectiveness of government work and aligning resources with priorities was most recently expressed in the Prime Minister's mandate letters to each of his ministers. Unlike other areas of democratic accountability, the security and intelligence community presents unique challenges because of the secrecy of its work. It is therefore important that Cabinet and ministers have measures in place to properly account for performance and expenditures as they relate to the intelligence priorities. This is a significant challenge facing the security and intelligence community in Canada and those among our allies, not least because of the difficulty in measuring success in a security and intelligence context.[31]

130. Efforts to improve accountability in intelligence began with a review of expenditures. In 2011, the Government initiated the National Security Expenditure Review. This review was designed to measure the spending and resources used to support the intelligence priorities. Organizational responses to the expenditure review varied considerably. The Government had requested expenditure information on how the departments and agencies were allocating money and resources to supporting the intelligence priorities. The first iteration, in 2012–2013, was coordinated by the Treasury Board Secretariat (TBS). TBS noted that the reporting from each department and agency showed no consistency in terms of what was measured and how, and that there was a lack of clear focus on distinguishing between spending on intelligence versus intelligence-led activities. Essentially, the information from the various organizations of the security and intelligence community could not be reconciled to provide a clear picture of expenditures on the intelligence priorities.

131. Early in the 2014–2016 cycle for setting the intelligence priorities, the community understood that it needed to establish the necessary standards, leadership, and processes needed for more robust horizontal intelligence expenditure and performance reporting.[32] In other words, the community needed to expand performance measurement beyond individual intelligence programs to include how intelligence is used throughout each organization. In 2015, the NSIA considered options for developing a system of performance measurement within the security and intelligence community in response to Government direction for more robust horizontal reporting. PCO informed the NSIA that,

> beyond providing high-level indications of responsiveness to strategic direction, the current reporting framework doesn't adequately [cover] how well or how efficiently [original emphasis] the community works in delivering on the priorities. This latter interpretation of performance is consistent with the Auditor General's 1996 recommendations to integrate performance

[31] United Kingdom, Intelligence and Security Committee of Parliamentarians, Annual Report 2016–2017, Section 10 Administration and Expenditure, pp.64-65.
[32] Privy Council Office, Security and Intelligence Secretariat, Assistant Secretary to the Cabinet, Presentation for Deputy Ministers' meeting, May 22, 2015.

reporting into the priorities process. The intent was to provide senior officials with additional tools to improve community performance in support of the priorities.[33]

132. PCO presented the NSIA with two options. One option was to create a full performance measurement framework that would explain the similarities and differences between the reporting of the organizations involved, but would also require more policy work and investment to implement and an increased leadership role for PCO. The other option was a simplified version focusing on responsiveness rather than performance that could be implemented within that cycle for setting the intelligence priorities.[34] The NSIA chose the latter option as it met Government requirements and was achievable within the time constraints of the cycle. This had implications for both expenditure and performance measurement, which the Committee discusses below.

Expenditures: What is the security and intelligence community spending?

133. The security and intelligence community provided the Committee information on financial expenditures and human resources. According to this information, the annual expenditure of the Government of Canada in support of the intelligence priorities is approximately ***, which supports approximately ***. The organizations captured by this data are CBSA, CSIS, CSE, DND/CAF, Global Affairs Canada, the Integrated Terrorism Assessment Centre, PCO, Public Safety Canada, and the RCMP. These organizations' expenditures to support the intelligence priorities account for just over *** percent of their total expenditures (approximately *** of $31 billion) because some of them have additional mandates and functions that are unrelated to intelligence.[35]

134. For expenditures, the updated system initiated in 2014 was developed by PCO, TBS, and Public Safety Canada, and implemented in 2016. The expenditure methodology was revised to demonstrate responsiveness, ensure greater consistency in financial reporting across departments, and better account for how much was being spent to support the intelligence priorities specifically. The changes were also intended to aid accountability and make reporting more consistent with other departmental financial reporting requirements. The review was renamed the National Intelligence Expenditure Review to reflect its emphasis on measuring only those activities and resources that support the intelligence priorities.

135. Notwithstanding these changes, the implementation of the new methodology was inconsistent across departments and agencies. For some departments, the new methodology led to positive change. DND/CAF developed a full methodology for calculating expenditures in support of the intelligence priorities, including methods for capturing relatively granular expenditure details (e.g., the number of aircraft-hours devoted to an intelligence function). For other organizations, the methodology for calculating the support for the intelligence priorities did not result in a corresponding breakdown of

[33] Privy Council Office, Briefing binder for incoming National Security and Intelligence Advisor on Intelligence Priorities, March 2015.
[34] Privy Council Office, Memorandum to NSIA – Scope of Reporting Associated with the GoC Intelligence Priorities Process (Decision Sought), April 1, 2015.
[35] Privy Council Office, National Intelligence Expenditure Report 2016–2017.

expenditures. For example, CSIS claimed 100 percent of its 2016–2017 budget as supporting the intelligence priorities based on its Departmental Results Framework.[36] Other process challenges included organizational delays in providing relevant information and confusion over differences in methodologies, issues that have been addressed by the community.[37]

136. These inconsistencies create challenges in evaluating the size and scope of the security and intelligence community. For example, when organizations over-report their expenditures on support to the intelligence priorities, the community cannot accurately assess, nor portray to Cabinet, the proportion of overall expenditures that are being spent on the government's intelligence priorities or the relative proportions spent on individual functions, such as assessment or collection. However, PCO notes that the validity of the numbers continues to improve and the community now has six years of annual financial data.[38]

Performance measurement: How well is the community doing?

137. Performance measurement continues to experience significant challenges. To respond to the 2014 decision to provide more comprehensive information, PCO developed a Performance Measurement Framework in 2015. As noted above, this was intended to measure how well and how efficiently the community was delivering on the intelligence priorities. Specifically, the draft framework identified four areas of importance:

- to provide information that could inform potential resource trade-offs within the community;
- to provide context for discussions on costs associated with different intelligence priorities and to understand how coordination and partnerships contribute to addressing the priorities rather than just examining the efforts of individual organizations;
- to provide clear measures of the capacity of each organization to address each priority and its ability to realign or shift its efforts when required to enable senior officials and Cabinet to consider significant gaps; and
- to provide insight into the community's capacity to disseminate intelligence in a timely and effective way to clients and the clients' capacity to manage and make the best use of the intelligence they receive.[39]

138. This proposed framework was part of the more comprehensive option for performance and expenditure measurement considered by the NSIA in 2015. The NSIA opted to proceed with more simplified reporting that focused on responsiveness to the intelligence priorities instead of performance, which was more easily implemented. As a result, this framework for establishing community standards

[36] CSIS, Meeting with DDG IAB, July 13, 2018; and CSIS, Response to NSICOP questions, June 2018. ("Security Screening Branch was included to align with the new Departmental Results Framework (DRF). As per the DRF, all Programs (including Security Screening) map to one Core Responsibility which is Security and Intelligence.")
[37] NSICOP Secretariat discussions with PCO, August 2018.
[38] Privy Council Office, Response to NSICOP Review of the National Intelligence Priorities, October 2018.
[39] Privy Council Office, Security and Intelligence Secretariat, Draft S&I Performance Measurement Framework (Background Only), April 24, 2015.

in performance measurement was never used. Instead, the community concentrated on measuring expenditures and production.

139. Measuring production (that is, the number of intelligence reports produced) without measuring performance to provide context presents challenges. Many organizations are faced with the challenge of counting production when reports cannot be easily categorized. While the practice of double (or multiple) counting is consistent with PCO direction, it results in considerable overlap in calculating production without any context to explain the discrepancies. While double counting may help the community and Cabinet identify where there is overlap in collection and assessment, it may also obscure how responsive the security and intelligence community is to specific priorities.

140. CSE sought to address this issue in 2015. That organization noted that, on average, 16 different intelligence requirements based on SIRs were identified for each report[40] – a flawed measurement of how well the organization was responding to the requirements and priorities. [*** The following text was revised to remove the names of specific priorities: For example, a long report on one priority may contain a single line referring to an organization but with no further context. That report would be automatically recorded as responding to both priorities, when in reality the intent of the report was the first priority.***]. In response, CSE implemented a tagging system whereby analysts identify the **intent** behind the reports by referencing specific SIRs. This allows CSE to provide metrics that reflect the intent of its reports, rather than relying on automated keyword associations. CSE also tracks its reports based on client feedback, including whether the report was read by at least one client, and whether it satisfied needs, was exceptional, or was actionable.[41] These methodologies combined to provide both quantitative and qualitative performance measurement of the value of the intelligence production.

141. This issue of measuring production without measuring performance to provide context affects other organizations as well. For example, the Intelligence Assessment Secretariat of PCO reported that it produced *** reports in 2017–2018. This is partially due to the Secretariat counting as a separate report each summary item within its *** (a document produced for senior government and political officials ***), and counting other single reports multiple times if they respond to more than one priority.[42]

142. The Committee was informed that the security and intelligence community continues to consider how to address these challenges and improve its capacity for measuring performance. The Committee understands that measuring performance in intelligence is difficult, a challenge faced by ***. PCO, which would coordinate such work, does not currently have the resources available to develop or implement substantial improvements. Nonetheless, performance measurement is important for accountability. Performance indicators give context to the expenditure information that the community provides to Cabinet for decision-making, which in turn supports the management of the community through identifying and understanding compromises, priorities, and areas for possible efficiencies.

[40] Communications Security Establishment, SIR Tagging – Background Information, 2015.
[41] Communications Security Establishment, Annual Report to the Minister of National Defence, 2013–2014, 2014–2015, 2015–2016, and 2016–2017.
[42] Intelligence Assessment Secretariat, "Distribution of Assessments per Standing Intelligence Priority," 2018

Conclusion

143. The Committee concludes that the process for setting the intelligence priorities is fundamental to ensuring accountability over an area of operations that is high in risk because of its sensitivity and potential impact on the rights of Canadians and because, of necessity, it is sheltered from public scrutiny. It is an essential mechanism to coordinate and maximize the activities and resources of the departments and agencies in the security and intelligence community. Indeed, the government establishes the priorities so that the departments and agencies can better determine where to expend their limited resources to collect, assess, and disseminate intelligence. Prioritization, compromise, and burden sharing are integral to the success of Canada's security and intelligence community, given its size and scope.

144. The Committee recognizes that improvements have been made in the process over the years. Given its importance, the process should be as robust as possible. This review has revealed a number of weaknesses:

- ministerial direction is not always promptly issued, consistent with the priorities, or fully implemented by organizations;
- the SIRs need to be reconciled with the capacity of the Canadian security and intelligence community;
- the community needs to ensure that Cabinet is receiving all relevant information to enable it to make decisions; and
- systems to track performance measurement are underdeveloped and systems to track financial expenditures inconsistent.

145. These issues are important and they should be addressed. Without a full understanding of limitations and weaknesses of intelligence, without full participation and engagement by participants, and without strong and consistent coordination and management, accountability is undermined. The Committee believes that its recommendations will contribute to a more robust and, ultimately, accountable process.

Findings

146. The Committee makes the following findings:

F1. The process for setting intelligence priorities has a solid foundation and overall participation by the community has made it more rigorous, inclusive, and systematically applied.

F2. Coordinating the timing and consistency of Ministerial Directions to organizations involved in the intelligence priorities process would add rigour to the process, strengthen the development of the Standing Intelligence Requirements, and increase the accountability of ministers.

F3. The great number of Standing Intelligence Requirements, particularly at the highest priority level, makes it difficult for the community to ensure that Cabinet has the information it needs on the significance of identified gaps in collection and assessment.

F4. In general, the internal processes that NSICOP examined were effective and enforced.

F5. The delay by CSIS in updating its internal Intelligence Requirements Document to incorporate the new intelligence priorities and SIRs in a timely manner undermined the accountability of both the Minister of Public Safety and Emergency Preparedness and Cabinet, and weakened the accountability of the overall system to support those priorities.

F6. The National Intelligence Expenditure Review methodology is not applied consistently by organizations to provide Cabinet with complete and comparable information on how organizational resources are used across government to respond to the intelligence priorities.

F7. Performance measurement for the security and intelligence community is not robust enough to give Cabinet the context it needs to understand the efficiency and effectiveness of the security and intelligence community.

Recommendations

147. The Committee makes the following recommendations:

R1. The National Security and Intelligence Advisor, supported by the Privy Council Office, invest in and take a stronger managerial and leadership role in the process for setting intelligence priorities to ensure organizational responses to the intelligence priorities are timely and consistently implemented.

R2. The security and intelligence community develop a strategic overview of the Standing Intelligence Requirements to ensure Cabinet is receiving the best information it needs to make decisions.

R3. Under the leadership of the National Security and Intelligence Advisor and supported by the Privy Council Office, the security and intelligence community develop tools to address the coordination and prioritization challenges it faces in relation to the Standing Intelligence Requirements.

R4. The security and intelligence community, in consultation with the Treasury Board Secretariat, develop a consistent performance measurement framework that examines how effectively and efficiently the community is responding to the intelligence priorities, including a robust and consistent resource expenditure review.

Chapter 4: Review of the Department of National Defence and the Canadian Armed Forces' Intelligence Activities

Introduction

148. The Committee reviewed the intelligence activities of the Department of National Defence/Canadian Armed Forces (DND/CAF) conducted in support of the defence mandate. This review is important for a number of reasons. Defence intelligence is critical to the success of CAF operations and the fulfillment of the DND/CAF mandate: for the defence of Canada; the defence of North America (with the United States); the promotion of international peace and security; and, supporting lawful requests from other government departments for defence intelligence support. The defence intelligence function in DND/CAF is largely unknown to Canadians. Furthermore, an independent, external review of the defence intelligence program has never been conducted. In terms of resources, the DND/CAF intelligence program is among the largest in the Canadian security and intelligence community and is forecast to grow over the next several years. It includes the full spectrum of intelligence activities, which means that DND/CAF may carry out all manner of intelligence activities, such as signals intelligence, human intelligence, counter-intelligence, and intelligence assessment.

149. Such intelligence activities are also carried out by other members of Canada's security and intelligence community, including the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), or the Royal Canadian Mounted Police (RCMP) – that have a legislative mandate tailored to their area of responsibility. While each organization has unique areas of responsibility, DND/CAF does not have the same kind of statutory structure supporting its intelligence activities; instead, it operates under an authority framework where defence intelligence activities are carried out under aspects of the *National Defence Act* and the Crown prerogative.

150. The previous chapter described many of the risks inherent in the conduct of intelligence activities. These risks include the disclosure of intelligence targets, causing damage to Canada's foreign relations, or the disclosure of intelligence sources, putting individuals at risk of physical harm. Like all intelligence activities, defence intelligence contains the same risks, albeit not always in the same areas and to the same degree as other organizations whose mandates touch more closely on the rights of Canadians.[1] The mitigation of these risks requires unique structures to support ministerial control and accountability.

151. The Committee did not conduct an in-depth examination of any specific area of defence intelligence activity. The breadth of the DND/CAF mandate and the scope of its intelligence activities are too broad for a single review. It first needed to gain an overall understand of defence intelligence activities. As a result, the Committee decided to limit its review to two parts. The first was an

[1] The Ministerial Directive on Defence Intelligence (see Appendix A) acknowledges that the conduct of defence intelligence activities can impact "the lives and/or legal or Constitutional rights of persons in Canada and Canadian citizens around the world, or . . . the rights of individuals more broadly as recognized by international law." The directive will be discussed in greater detail later in this chapter.

exploration of the types of intelligence activities conducted by DND/CAF and the structure of its intelligence organization. The second was an examination of the authorities under which DND/CAF intelligence activities are conducted. The Committee believes that this review will help improve Canadians' and Parliament's awareness and knowledge of the DND/CAF defence intelligence mandate and activities. It can also set the stage for future reviews by the Committee and by the proposed National Security and Intelligence Review Agency (NSIRA).[2]

152. Following an initial DND site visit in March, the Committee started its review in April 2018. The initial focus was on three questions:

- What are the DND/CAF intelligence activities?
- Under what authorities are these activities conducted?
- To what accountability mechanisms are these activities subject?

153. Between April 27 and December 4, 2018, the Committee received and reviewed more than 4,500 pages of material from DND/CAF (both classified and unclassified), including legal opinions, ministerial letters, ministerial directives, functional and operational guidance documents, training manuals, briefing notes, presentations, operational authorizations and directions, and intelligence reporting. It also received numerous written responses and working-level briefings, including in the development and use of sensitive defence intelligence capabilities; legal authorities and the Crown prerogative; human intelligence; and counter-intelligence. The Committee supplemented this material with separate academic and legal research.

154. In addition to two general briefings on the role and activities of DND/CAF, the Committee received four specific briefings from DND/CAF officials during this review. The first was on the Crown prerogative and its use in authorizing the development and use of defence intelligence capabilities in CAF operations. The second was on the central role that defence intelligence plays in planning and conducting operations, which focused on the full spectrum of DND/CAF intelligence activities ***. The third and fourth were on the question of providing DND/CAF with an explicit statutory mandate for defence intelligence activities.

155. The Committee received information from other government departments. This included CSE regarding the Ministerial Directive on the Integrated SIGINT [Signals Intelligence] Operations Model, which establishes the framework under which CSE delegates to CAF its authority to collect foreign intelligence ***; the Department of Justice regarding the Crown prerogative and authority for defence intelligence; Global Affairs Canada regarding interdepartmental consultations with DND/CAF on ***; and CSIS regarding its engagements with DND/CAF *** pursuant to section 12 of the *CSIS Act*.

156. This chapter details the Committee's findings. It discusses DND/CAF defence intelligence activities and how they support CAF operations from early deployment planning through to the day-to-

[2] Bill C-59, Third-Reading, subsection 8(1)(*b*), where the NSIRA mandate is to review any activity carried out by a department that relates to national security or intelligence. www.parl.gc.ca/DocumentViewer/en/42-1/bill/C-59/third-reading. Accessed July 27, 2018.

day conduct of military operations. It describes how defence intelligence activities are authorized and conducted domestically and internationally. It also describes the internal administrative system developed by DND/CAF with respect to the governance of intelligence activities. This system consists of ministerial direction, ministerial authorization, internal oversight committees, internal reviews, policy, administrative orders, and doctrine.[3] This system is also bolstered by statutory obligations stemming from the chain of command, which DND/CAF describes as a system of command and control applicable to CAF members, pursuant to subsection 18(2) of the *National Defence Act* and the Code of Service Discipline (Part III of the *National Defence Act*). This system of command and control obligates CAF members to comply with lawful orders and directions and is described by DND/CAF as a foundational element through which the accountability and compliance of defence intelligence activities are maintained.[4]

157. The defence intelligence program is a legitimate part of the DND/CAF mandate for the defence of Canada and Canadian interests abroad. The Committee recognizes that, at any given time, the Government can call upon the CAF to undertake missions for the protection of Canada and Canadians and to maintain international peace and stability, and that defence intelligence activities are an integral part of ensuring the success of DND/CAF missions and operations. Paragraph 170 of this chapter lists DND/CAF defence intelligence activities and their use as part of the defence mandate.

158. The Committee recognizes that DND/CAF's administrative system of governance over defence intelligence activities is an important component of risk mitigation for intelligence operations and to ensure appropriate control and accountability over defence intelligence activities. That said, the Committee identified weaknesses in that system. These include: a lack of standardized processes for determining a 'nexus' between the use of a defence intelligence activity and a legally authorized mission of the CAF, and for interdepartmental consultations regarding the use and deployment of sensitive defence intelligence activities; limited formal measurement of compliance with Ministerial Direction by the principal oversight body within DND/CAF; and gaps in existing external review of defence intelligence activities. The Committee believes that these weaknesses undermine the system of governance and accountability that DND/CAF has implemented over defence intelligence activities. The Committee makes four findings and three recommendations.

159. This chapter begins by detailing the rationale behind the Committee's decision to conduct a review of DND/CAF defence intelligence activities. The chapter continues with a discussion of the

[3] DND, *Canadian Forces Joint Publication 01 – Canadian Military Doctrine*, April 2009. Doctrine is defined as "the fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgement in application." For DND/CAF, the creation and application of doctrine describes the relationship between the CAF and the Government of Canada, including: national security and strategic policy applicable to the CAF; the constitutional, political, legal and administrative context within which Canada may use military power; and the application of military power within Canada and the North American continent for domestic purposes. http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

[4] DND, *Canadian Forces Joint Publication 01 – Canadian Military Doctrine*. April 2009. *Command and Control* within the chain of command is defined as "the authority, responsibilities and activities of military commanders in the direction and coordination of military forces and in the implementation of orders related to the execution of operations." http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

authorities under which defence intelligence activities are conducted, and closes with a discussion of the benefits and risks of placing defence intelligence activities under statute.

Background: The rationale for review

Importance of increasing public knowledge of defence intelligence activities

160. The Committee's decision to conduct a review of defence intelligence was based on a number of considerations. The first was that the defence intelligence program within DND/CAF has not received the same parliamentary or public attention as other aspects of DND/CAF activities, or as other intelligence organizations, that is, CSIS and CSE. This gap is reflected in academic research on defence intelligence in Canada. As Canadian academic Wesley Wark noted in his study of the evolution of military intelligence in Canada, "the almost nonexistent state of literature on the history of Canadian military intelligence and the fragmentary nature of the available archival record rule out documenting this [evolution] in full detail."[5] The same is true of other Westminster governments, such as the United Kingdom:

> [Defence Intelligence has not] yet experienced the levels of public or academic . . . interest or concern that has propelled the enthusiastic scrutiny of the national agencies and Cabinet Office central intelligence machinery. . . .Intelligence scholarship is at the point of little more than a first pass or two at the question of defence intelligence in the UK, and this represents barely a scratch on the surface of the far larger question of the role and status of defence intelligence institutions globally and comparatively. Even in the British case, the unexplored territory remains daunting in its scale.[6]

DND/CAF resources devoted to defence intelligence

161. The second consideration was that the DND/CAF intelligence program is among the largest in Canada. According to the National Intelligence Expenditure Review, discussed in Chapter 3 of this report, DND/CAF expenditures in support of Government of Canada intelligence priorities were the *** in Canada in 2016–2017 at *** (CSIS spent $582 million). This figure represented nearly *** percent of the total recorded departmental expenditures of just over $19 billion.[7] The same is true for human resources: the number of full-time employees DND/CAF devoted to government intelligence priorities was *** (CSIS had ***), with an additional *** personnel devoted to work in other areas of the DND/CAF intelligence program (for a total of *** personnel). DND/CAF has an additional *** unstaffed intelligence positions and is expected to increase its human resources by a further 300 personnel under the Defence Policy, *Strong, Secure, Engaged*.

[5] Wesley Wark, "The Evolution of Military Intelligence in Canada," *Armed Forces and Society*, Vol. 16, no. 1, Fall 1989, pp. 77–98. A few papers have been published since 1989. See Daniel Villeneuve, "A Study of the Changing Face of Canada's Army Intelligence," Canadian Army Journal, Vol 9, No. 2, Summer 2006, pp. 18-36; J.A.E.K. Dowell, "Intelligence for the Canadian Army in the 21st Century," JADEX Papers, 5, National Defence, July 2011; David A. Charters, "Canadian Military Intelligence in Afghanistan," International Journal of Intelligence and Counterintelligence, Vol 25, no. 3, 2012, pp. 470-507.

[6] Philip H. J. Davies, Myron Varouhakis, and Neveen Abdalla, "Defence Intelligence in the UK: an agenda for inquiry within and beyond the '3 mile limit,' " *Intelligence and National Security*, 31:6, 2016, pp. 793–796.

[7] DND, Chief of Defence Intelligence/Commander, Canadian Forces Intelligence Command, Letter attesting to the 2016–2017 DND/CAF National Intelligence Expenditure Review submission, August 29, 2017.

Authorities for the full spectrum of defence intelligence activities

162. The third consideration was that DND/CAF conducts a broader range of intelligence activities than any other Canadian intelligence organization. The Defence Policy describes the Canadian Forces Intelligence Command as "the only entity within the Government of Canada that employs the full spectrum of intelligence collection capabilities while providing multi-source analysis." It commits to build these capabilities further. Many of the defence intelligence activities conducted in support of DND/CAF operations are similar to activities conducted by CSIS, CSE, and the RCMP, specifically activities in the areas of human intelligence, signals intelligence, counter-intelligence, open-source intelligence, and ***.[8] As paragraph 221 outlines, these are also the defence intelligence activity areas that DND/CAF has defined as sensitive. While these activities are similar or identical, they are conducted in accordance with each agency or department's respective legislative mandate and authorities. In this context, the Committee wanted to better understand the authorities under which DND/CAF conducts its activities.

Risks associated with intelligence activities

163. The fourth consideration was the risks that intelligence activities entail. Intelligence is almost always classified in order to protect sources and methods. The disclosure of an intelligence target, such as a foreign state, could cause significant damage to Canada's foreign relations. The disclosure of a source or a method of collection could put an individual at risk of physical harm or could lead targets to change their behaviour, causing a loss of vital intelligence and potentially significant resources that were invested to obtain access to that source. Intelligence activities may also affect the rights of Canadians through, for example, intrusive investigative methods or through the sharing of information (or intelligence), which may lead to improper treatment. The magnitude of this risk is reflected in the 2018 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities.[9] The Committee wanted to better understand how these risks are mitigated in the DND/CAF context.

The absence of independent external review of defence intelligence

164. The fifth consideration was that the DND/CAF intelligence program is not subject to independent, external review.[10] The Committee believes that independent, external review of security and

[8] Paragraph 170 further defines and delineates these and other defence intelligence activity areas.

[9] Government of Canada, Ministerial Direction to the Department of National Defence and the Canadian Armed Forces: Avoiding Complicity in Mistreatment by Foreign Entities, www.canada.ca/en/department-national-defence/corporate/ministerial-directions/avoiding-complicity.html; and Government of Canada, *Statement from Minister Goodale on bringing openness, transparency, and clarity to new Ministerial Directions*. www.canada.ca/en/public-safety-canada/news/2017/09/statement_from_ministergoodaleonbringingopennesstransparencyandc.html.

[10] NSICOP recognizes that the Office of the Communications Security Establishment Commissioner has twice reviewed one aspect of DND/CAF defence intelligence activities, CAF signals intelligence activities. In 2009, the Commissioner reviewed certain CSEC foreign intelligence collection activities conducted under two successive ministerial authorizations and in support of government efforts relating to Afghanistan (2006-2007 and 2007-2008); and, in 2015 the Commissioner reviewed the Canadian Armed Forces Cyber Support Detachment. In both reviews, the CSE Commissioner found that these activities were in compliance with the law and relevant CSE operational policy instruments. https://www.ocsec-bccst.gc.ca/s21/s51/eng/classified-reports-submitted-Minister. Accessed October 16, 2018. In 2009, the Auditor General made reference to defence intelligence, focused specifically on the changes to the structure of the defence intelligence program and the creation of the Canadian Forces Intelligence Command, and improvements to the internal control of defence intelligence that resulted. The Report was not, however, an in-depth examination of the DND/CAF defence intelligence program, nor any

intelligence activities is a foundational part of improving public confidence and trust in the activities of security and intelligence agencies. Review enhances accountability and transparency. Independent, external organizations have reviewed CSIS and CSE activities for some time. Their experience shows that review improves the operations of the reviewed organizations and increases the trust of Canadians that security and intelligence agencies act in accordance with the law, are accountable for their actions, and respect Canadians' rights and freedoms. The Committee's decision to conduct an exploratory review of DND/CAF intelligence activities would help to address the gap in independent external review.

---

one area of intelligence activity. *2009 March Status Report of the Auditor General of Canada*. http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_01_e_32288.html.

Defence intelligence: Definitions, structure, and activities

165. In this review, the Committee's objective was to understand **what** intelligence is in the DND and CAF context, **who** conducts intelligence activities, and **how**, **where**, and **by whom** it is used. This section provides relevant definitions and describes the structure and activities of defence intelligence. The next section describes the authorities under which those activities are conducted.

166. DND/CAF defines intelligence broadly. The Defence Policy identifies the role of intelligence in all aspects of national defence decision-making, describing intelligence as fundamental to the conduct of any domestic or international operation.[11] At its broadest level, defence intelligence is defined as encompassing "all intelligence activity conducted by or within the DND and the CAF, and [including] joint, maritime, land, air, space and cyber intelligence, from the tactical to the strategic level (as well as the geopolitical, economic, scientific, technical and security intelligence [level]) where such intelligence supports the defence mission and the Government of Canada's broader responsibilities as it relates to national defence, national security and foreign affairs."[12]

167. More specifically, DND/CAF defines intelligence and defence intelligence as:

- **Intelligence:** the product resulting from processing information concerning foreign nations, hostile (or potentially hostile) forces, or areas of actual or potential operations. The term 'intelligence' is also applied broadly to intelligence activities that result in the product (for example, an intelligence report), and to the organizations engaged in intelligence activities.[13]
- **Defence Intelligence:** all intelligence in support of military objectives and planning, either international or domestic, and including strategic, operational, and tactical intelligence for a spectrum of activities from the formulation of military policies, plans, and direction, to a commander's understanding of adversarial capabilities and intentions, to specific threats and hazards a commander may face in achieving a specific mission or objective.[14]

168. DND/CAF also defines three levels of intelligence: strategic, operational, and tactical. These levels support the formulation of military policies and plans to inform Government decision-making and to achieve strategic objectives; provide the detailed information required to broadly plan military operations; and support the ongoing use of military forces to achieve specific objectives when deployed.[15]

[11] "Enhancing Defence Intelligence," *Canada's Defence Policy – Strong, Secure, Engaged*, pp. 65–66, accessed at: http://dgpapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.
[12] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017.
[13] DND, Defence Administrative Order and Directive (DAOD) 8008-0, "Defence Intelligence"; and Joint Doctrine Branch Canadian Forces Warfare Centre,*Canadian Forces Joint Publication (CFJP) 2.0 Intelligence*, October 2011.
[14] DND, DAOD 8008-0, "Defence Intelligence"; and Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations.*
[15] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017.

The defence intelligence program

169. The DND/CAF intelligence program currently employs more than *** personnel (regular force, reserve force, and civilian) from within an allotted staffing envelope of nearly *** positions. These personnel are spread across the constituent elements of the Defence Intelligence program: the National Intelligence Organizations, the CAF Services, and the Environmental Commands:[16]

National Intelligence Organizations:

- Chief of Defence Intelligence (CDI): As the functional authority for defence intelligence,[17] responsible for providing intelligence advice; generating specialist intelligence personnel, equipment, and connectivity for CAF operations; and ensuring defence intelligence activities are carried out in a responsive, efficient, and accountable manner.
- Canadian Forces Intelligence Command: Responsible for providing strategic intelligence advice, products, and services; developing future defence intelligence capabilities; and generating specialist intelligence personnel, equipment, and connectivity for operations.
- Canadian Forces Information Operations Group: Responsible for the coordination, development, and employment of capabilities for the collection and production of signals intelligence.

CAF Services:

- Royal Canadian Navy: Maintains operational intelligence support for deployed maritime forces.
- Canadian Army: Maintains land intelligence staff within the Canadian Army staff at National Defence Headquarters and within its divisional headquarters; also includes an intelligence regiment, an electronic warfare regiment, and five reserve companies.
- Royal Canadian Air Force: Maintains an air intelligence staff at Headquarters, within several air divisions, many wings, and some squadrons.

Environmental Commands:

- Canadian Joint Operations Command: Responsible for all operations, except those conducted solely by Canadian Special Operations Forces Command elements under the direct authority of the Chief of the Defence Staff.
- Canadian Special Operations Forces Command: Responsible for all special operations, including responding to terrorist threats to Canadians and Canadian interests around the world.
- North American Aerospace Defence Command (NORAD): Responsible to the Canadian and United States governments for the execution of missions assigned to NORAD, including aerospace warning, aerospace control, and maritime warning.

[16] DND, Canadian Forces Intelligence Command, Defence Intelligence Overview, Deck, April 2018; and Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017.
[17] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017. A functional authority: sets standards, communicates clear expectations, issues binding functional direction, offers non-binding functional advice and guidance, consults and obtains feedback, monitors to ensure compliance with direction, and creates a management framework whereby the Deputy Minister and the Chief of the Defence Staff can hold senior commanders and advisors across the organization accountable for compliance.

Defence intelligence activities

170. DND/CAF maintains a large defence intelligence program that includes a range of intelligence activities. DND/CAF describes these activities as essential in establishing comprehensive situational awareness for the protection of deployed forces, DND installations, and personnel, and for supporting the achievement of mission objectives in all operational environments. DND/CAF's current defence intelligence activities include:[18]

- **Signals Intelligence (SIGINT):** Derived from the interception, collection, processing, and analysis of communications and data links, including email, mobile, and telephone communications. SIGINT also includes intelligence derived from electromagnetic emissions and instrumentation signals from things such as radar, missile guidance, and command systems.[19] As a practical example, [*** This section describes an example of how SIGINT was used in support of an operation. ***].[20]
- **Imagery Intelligence:** Derived from the collection and analysis of hand-held and satellite imagery (for example, mapping data or bomb damage and data assessments using imagery).
- **Geospatial Intelligence:** Derived from the collection and analysis of various geomatics' sensors and data, including analysis of maps, charts, or nautical information for intelligence purposes. As a practical example, geospatial and imagery intelligence [*** This section describes an example of how geospatial intelligence was used in support of an operation.***][21]
- **Human Intelligence (HUMINT):** Derived from the collection and analysis of information from human sources. HUMINT activities are conducted by specialized units and include ***, and the interrogation of detained individuals. DND/CAF also defines HUMINT activities to include the normal interaction of CAF members with a local population on deployment, the overt diplomatic engagement with foreign counterparts conducted by its defence attaches, and structured interviews of specific Canadians by CAF HUMINT personnel.[22] As a practical example, [*** This section describes an example of how HUMINT was used in support of an operation.***].[23]
- **Counter-Intelligence:** Activities concerned with identifying and countering threats to the security of DND/CAF personnel, property, and information by hostile intelligence services, organizations, or individuals. DND/CAF describes its efforts in this area as entailing "the full-spectrum of [counter-intelligence] activities for the purpose of identifying threats to the security of DND/CAF."[24]

[18] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017; and DND, CDI Functional Directive: ***.

[19] SIGINT collection is performed in the Canadian intelligence community by both CSE, under Part A of its mandate (foreign intelligence), and by DND/CAF as part of *** delegated CSE authorities. Information briefing to the NSICOP Secretariat on the Integrated SIGINT Operations Model, July 23, 2018.

[20] DND, Defence Intelligence Support to Operations, Deck presented to NISCOP, August 14, 2018.

[21] DND, Defence Intelligence Support to Operations, Deck presented to NISCOP, August 14, 2018.

[22] DND, Chief of Defence Intelligence Functional Directive: CAF Policy Framework for the Conduct of HUMINT Activities.

[23] DND, Defence Intelligence Support to Operations, Deck presented to NISCOP, August 14, 2018.

[24] Joint Doctrine Branch Canadian Forces Warfare Centre, Canadian Forces Joint Publication (CFJP) 2.0 Intelligence, October 2011; and DND, CDI Functional Directive: Counter-Intelligence Investigations – Preliminary Assessments and Level 1 Subject Interviews; and Defence Administrative Order and Directive (DAOD) 8002-0, Counter-Intelligence. According to DND/CAF documentation, the "full spectrum" of CI activities does not mean that DND/CAF authority for counter-intelligence activities, especially in the domestic context, supersedes the authorities of domestic law enforcement or security agencies. DND/CAF

- **Measurement and Signatures Intelligence:** Derived from the collection and analysis of signatures (unique characteristics) of fixed and dynamic targets (for example, ***).
- **Technical Intelligence:** Derived from information concerning the capabilities and operation of foreign technology that may have a practical military application. This can include ***.
- **Medical Intelligence:** Derived from the study of medical, bio-scientific, epidemiological, and environmental information for the purpose of protecting deployed forces. This can include analysis of the impact of disease and environmental hazards on military forces.
- **Meteorology–Oceanography:** Derived from the study of atmospheric chemistry and physics (weather) and physical and biological aspects of the ocean. This deals predominantly with the environmental impact of climatic conditions on personnel, platforms, weapons, sensors, communications, and mission planning.
- **Open-Source Intelligence:** Derived from the press and other media, reference material, journals, publications, and other unclassified material.
- [*** This section describes a specific intelligence activity. ***]

notes that authority for criminal investigations of threats to the security of DND/CAF rests with the police or security agency of jurisdiction, which would lead any DND/CAF investigation.

Defence intelligence authorities

171. The previous section defined intelligence in the DND/CAF context and described the structure of the DND/CAF defence intelligence program and its activities. This section focuses on the authorities under which DND/CAF conducts its defence intelligence activities and how those authorities support departmental and ministerial accountability for their use.

172. In the most general terms, the authority to create military forces is found in the *Constitution Act, 1867*, which assigns the federal Parliament legislative authority over defence. Parliament has exercised this authority by adopting the *National Defence Act*, which gives the Minister of National Defence the management and direction of the CAF and all matters relating to national defence. For specific deployments of military forces, the Government authorizes the use of the CAF through a decision by the Prime Minister, Cabinet, or one or more ministers (this decision is referred to as an exercise of the Crown prerogative, itself a source of legal authority that is described below). The authority to conduct defence intelligence activities comes from the specific decision to deploy military forces. As DND/CAF notes, "The authority to conduct defence intelligence activities is **implicit** when the CAF is legally mandated, pursuant to legislation or an exercise of the Crown Prerogative, to conduct military operations and other defence activities." [emphasis added][25] Neither the *National Defence Act* nor any other statute contains provisions that specifically govern the conduct of defence intelligence activities by DND/CAF.

173. The deployment of the CAF, which includes the conduct of defence intelligence activities, is governed and constrained by Canadian and international law. The CAF Judge Advocate General put it simply in her remarks to the Committee:

- All CAF operations are authorized by law.
- All CAF operations are conducted in accordance with the law; and while the sources of legal authority will vary depending on the type of mission:
  - all domestic operations must have a legal basis in Canadian law and be conducted in accordance with Canadian law; and
  - all international operations must have both a legal basis under Canadian law and a legal basis under international law. They must also be conducted in accordance with both Canadian law and with the applicable international law.[26]

[25] DND, ***, April 27, 2018.
[26] DND, Oral remarks of the Judge Advocate General to NSICOP, June 19, 2018.

Authorities for defence intelligence activities conducted in Canada

174. Defence intelligence activities support CAF domestic operations in the Canadian Area of Operations (which includes Canada's territorial waters and land, including in the Arctic). These operations are authorized either by statute or an exercise of the Crown prerogative (discussed in detail below). Domestic operations are conducted to:

- **Assert Canada's sovereignty:** The CAF detects and deters the activities of foreign states or hostile entities directed toward actual or potential attack, or other acts of aggression against Canada. As an example of intelligence used to support such operations, the CAF may intercept radio communications of *** aircraft approaching Canadian airspace, permitting the Air Force to intercept them as they approach Canada.
- **Respond to requests for assistance by civil authorities:** The CAF responds to requests for assistance from civil authorities, in cases such as natural disasters or emergencies. These operations are subject to Canadian laws, including the *National Defence Act*. For example, the CAF may conduct overflights as part of preparations to respond to requests for assistance in battling forest fires.
- **Identify and counter threats to the security of DND employees, CAF members, and DND and CAF property and information:** DND/CAF identifies and counters threats posed by hostile intelligence services, organizations, or individuals that may engage in espionage, sabotage, subversion, terrorist activities, organized crime, and other criminal activities.[27] For example, the CAF counter-intelligence unit may investigate a soldier who has suspicious links to a foreign state.

175. Where intelligence activities are used to support such domestic operations, their scope is circumscribed by law, by the specific responsibilities of various departments and agencies, and by the balance of jurisdiction between federal and provincial authorities. In terms of domestic legislation, DND identified several significant sources of law, including:[28]

- **The *National Defence Act*:** Subsection 273.6 of the Act permits DND/CAF to provide public service and assistance to law enforcement, and Part VI of the Act defines when the CAF can come to the Aid of the Civil Power (that is, to respond to riots or disturbances of the peace that cannot be handled without the assistance of CAF).[29]
- **The *Canadian Charter of Rights and Freedoms*:** DND/CAF intelligence activities must not violate the provisions of the Charter, particularly section 7 (the right to life, liberty, and security of the person) and section 8 (the right against unreasonable search and seizure).

[27] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.0 Intelligence*, October 2011; and Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017.

[28] DND, ***, April 27, 2018; Office of the Judge Advocate General, *The Law of Interrogations. The Issue of Torture and Ill-treatment*, Strategic Legal Paper Series, Issue 1, 2008; and DND, ***, July 18, 2003.

[29] Blaise Cathcart, a former Judge Advocate General, recently commented that the last time Part VI of the *National Defence Act* was used was in response to the Oka crisis in 1990: Blaise Cathcart, Comments during an appearance on the Intrepid Podcast, "A Podcast Called Intrepid." www.intrepidpodcast.com/podcast/2018/7/25/ep-47-calling-in-the-big-guns. Accessed August 19, 2018.

- **The *Criminal Code*:** DND/CAF intelligence activities must not violate the *Criminal Code*, including sections dealing with search warrants and the interception of private communications.
- **The *Access to Information Act* and *Privacy Act*:** DND/CAF intelligence collection activities and storage practices must comply with the provisions of the *Access to Information Act* and the *Privacy Act*.

176. In most cases, CAF domestic operations are conducted in support of other government departments and agencies and at the formal request of their minister. In such cases, these operations, including defence intelligence activities, are conducted pursuant to the legal authorities of the supported entity. As the CAF Judge Advocate General stated, this means, "When acting in support of another organization, the Canadian Armed Forces has no more powers than those of the supported agency."[30] In short, the CAF can conduct an intelligence activity (for example, intercept radio communications) only to support another government department (for example, the RCMP) if that department itself has the authority (for example, a court warrant) to conduct that activity.

177. To illustrate how these authorities and constraints work in practice, DND/CAF provided legal opinions specific to the defence intelligence legal framework, and operational examples of domestic operations. The first example was in regard to intelligence assistance for [*** This text refers to an event in Canada***]. In this case, the Solicitor General (now the Minister of Public Safety and Emergency Preparedness), on behalf of the RCMP, requested "the use of [DND/CAF] personnel and equipment in support of the RCMP in its law enforcement security duties [*** This section describes the type of assistance sought by the RCMP, and the result which was that the assistance was not provided.***]."[31] The second example was DND/CAF assistance for the [*** This text refers to an event in Canada***]. In that case, the Minister of Public Safety and Emergency Preparedness requested that the CAF provide support to the RCMP, including intelligence related to ***. The Minister of National Defence agreed to provide assistance pursuant to subsection 273.6 of the *National Defence Act*.

Authorities for defence intelligence activities conducted in international operations

178. Defence intelligence activities in support of CAF international operations are subject to similar constraints. Generally, DND noted that the specific instrument of domestic or international law that may affect a defence intelligence activity varies by circumstance. These circumstances include the location of an operation; whether it is conducted under the auspices of an invitation from a foreign state or under the auspices of a United Nations resolution; whether the operation is conducted in relation to a recognized international armed conflict, to which specific instruments of international law and international humanitarian law apply; and whether a particular activity is recognized as contrary to international law or international humanitarian law. In short, the legal instrument that affects the conduct of an intelligence activity varies by the circumstances of the mission.

179. Canadian law follows the CAF. Whether employed in Canada or deployed on operations abroad, CAF personnel are subject to the Code of Service Discipline (which delineates service offences and

[30] DND, Remarks of the Judge Advocate General, to NSICOP. June 19, 2018.
[31] DND, ***, June 4, 2002.

includes any offence under any federal statute, in accordance with section 130 of the *National Defence Act*).[32] This means that if a CAF member commits a service offence abroad, he or she may be charged and tried in Canada's military justice system. The CAF is also subject to instruments of international law that could involve defence intelligence activities, including:

- the *United Nations Charter*;
- the *Geneva Conventions*; and
- the *Law of Armed Conflict*.

180. To illustrate how these authorities and constraints work in practice, DND/CAF provided operational examples from the CAF deployment ***. The first example, SIGINT activities in international operations, speak to the manner in which Canadian law follows the CAF. When deployed, the CAF collects SIGINT [*** This text provides an example and some objectives of the use of SIGINT.***] The authority to conduct this foreign intelligence activity is found in Canadian domestic legislation, specifically Part V.1 of the *National Defence Act* (Communications Security Establishment), which is the statutory basis of CSE. For deployed operations, the Minister of National Defence has delegated the authority to conduct SIGINT activities from CSE to the CAF through the Ministerial Directive on the Integrated SIGINT Operations Model. This means that CAF SIGINT activities are subject to the same restrictions as CSE authorities under Part V.1 of the *National Defence Act*,[33] including that they cannot be directed at Canadians, are subject to relevant ministerial authorizations, and are subject to review for lawfulness by the Office of the CSE Commissioner.[34] In short, the CAF authority to conduct SIGINT activities *** derives from the Government's decision to deploy forces ***; the actual conduct of those activities is shaped (in this case, both enabled and limited) by Canadian domestic legislation, ministerial direction, and ministerial authorization.

181. The second example, CAF HUMINT activities ***, speaks to the manner in which CAF activities are subject to instruments of international law. In that context, a *** HUMINT *** provides intelligence that may help fulfill the objectives of the CAF mission, such as [*** This text provides some objectives of the use of HUMINT. ***]. CAF HUMINT activities are subject to operational doctrine, which references sources of international law, such as the *Protocols to the Geneva Conventions*, which prohibits the recruitment and use of children in hostilities, for example as intelligence sources or agents.[35] Like the authority for the CAF to conduct SIGINT activities, the authority to conduct HUMINT activities is derived

[32] DND, Written submission to NSICOP, November 19, 2018.

[33] In the Canadian intelligence community SIGINT collection is performed by both CSE under Part A of the CSE mandate (foreign intelligence) and by the DND/CAF as part of *** delegated CSE authorities. Information briefing to the NSICOP Secretariat, "Integrated SIGINT Operations Model," July 23, 2018. CSE noted that CAF also conducts SIGINT activities under CSE authorities that are not done directly in support of deployed operations (e.g., ***).

[34] Not every annual report from the Office of the CSE Commissioner covers the activities of the Canadian Forces Information Operations Group. CAF signals intelligence activities are not, as a rule, all reviewed by the CSE Commissioner – they are, however, *subject* to review by the Commissioner. CSE, Written submission to NSICOP, October 1, 2018.

[35] DND, Chief of Defence Intelligence Functional Directive: CF Policy Framework for the Conduct of HUMINT Activities. International Humanitarian Law prohibits the participation of child soldiers in hostilities, and in activities involved in military intelligence such as scouting, spying, sabotage, and the use of children as decoys, couriers or at military checkpoints. *International Committee of the Red Cross. International Humanitarian Law Database of Customary International Humanitarian Law, Rule 137: Participation of Child Soldiers in Hostilities.* https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule137.

from the Government decision to deploy forces ***. The actual conduct of HUMINT activities must be authorized by the Minister of National Defence in each case and is limited by specific sources of domestic and international law (such as the *Additional Protocols to the Geneva Conventions*).[36]

NSICOP assessment

182. The Committee recognizes that DND/CAF conducts defence intelligence activities under a unique and complex authority structure. At its simplest, the DND/CAF authority to conduct intelligence activities derives from the Government's exercise of the Crown prerogative to deploy the CAF. DND/CAF conduct of those activities is governed by domestic (i.e., section 273.6 and Part VI of the *National Defence Act*) and international legal instruments; ministerial direction and ministerial authorization; the DND/CAF internal administrative governance system of policies, procedures, and functional directives; and orders given through the military chain of command. The Committee turns next to an examination of the nature and use of the Crown prerogative and the content of DND/CAF's existing administrative structure of governance for defence intelligence activities.

[36] DND, Written submission to NSICOP, July 4, 2018. It is important to emphasize that ministerial authorizations to obtain foreign intelligence are a statutory authority found in Part V.1 of the *National Defence Act* (Communications Security Establishment), which authorize CSE and, through delegated authority, the CAF, to intercept private communications under specific conditions. In contrast, ministerial authority for CAF HUMINT activities flows from the Crown prerogative.

What is the Crown prerogative?

183. In addition to the authorities provided by the *Constitution Act, 1867*, and the *National Defence Act*, the main source of authority for the deployment of the CAF, and the derivative authority for the conduct of associated defence intelligence activities, is known as the Crown prerogative. The Crown prerogative is a source of executive power and privilege accorded by common law to the Crown.[37] British constitutional theorist A. V. Dicey describes the Crown prerogative as the "residue of discretionary or arbitrary authority, which at any time is left in the hands of the Crown."[38] Put simply, the Crown prerogative is the authority exercised by the government to make decisions in areas where the prerogative has not been displaced, or otherwise limited, by Parliament through the enactment of statute, or by the courts.

184. The Crown prerogative is not unlimited. In the Canadian context, the Privy Council Office has tracked the degree to which the Crown prerogative has been reduced over time by Parliament through legislation, noting that "the history of parliamentary government has been a process of narrowing the exercise of the prerogative authority by subjecting it increasingly to the pre-eminence of the statutory authority, substituting the authority of the Crown in Parliament for the authority of the Crown alone."[39] As the Supreme Court of Canada has observed, "[o]nce a statute occupies the ground formerly occupied by the prerogative power, the Crown must comply with the terms of the statute."[40] A recent and relevant example of the Crown prerogative being displaced by Parliament in an area of intelligence is the continuance of CSE in legislation. Prior to 2001, CSE had conducted its activities under the Crown prerogative authority of two orders in council.[41] In December 2001, Parliament passed the *Anti-terrorism Act*, which amended the *National Defence Act* to incorporate in statute the mandate, authorities, and legal limitations of CSE's activities.

185. Court decisions have further constrained the Crown prerogative in a variety of ways. Until recently, the exercise of prerogative powers was subject to judicial review only on very narrow grounds – if a prerogative power was asserted, courts would determine whether such power actually existed, its extent, and whether it had been displaced or limited by statute. In the last decades, the scope of judicial review of prerogative powers has expanded as a consequence of the passage of the *Canadian Charter of Rights and Freedoms*, after which the Supreme Court of Canada ruled that executive decisions, including exercises of the Crown prerogative, were amenable to judicial review under the Charter where they

[37] Peter W. Hogg, *Constitutional Law of Canada*, Looseleaf ed. (Scarborough: Thomson Carswell, 1997) at 1.9, note 76.
[38] *Reference as to the Effect of the Exercise of the Royal Prerogative of Mercy Upon Deportation Proceedings*, [1933] S.C.R. 269, at p. 272, per C. J. Duff, quoting A . V. Dicey, *Introduction to the Study of the Law of the Constitution*, 8th ed., 1915, p. 420.
[39] Privy Council Office, *Responsibility in the Constitution*, www.canada.ca/en/privy-council/services/publications/responsibility-constitution.html. Accessed November 20, 2018. Also cited in Craig Forcese, *The Executive, the Royal Prerogative and the Constitution*. In Peter Oliver, Patrick Macklem, and Nathalie Des Rosiers, eds., *The Oxford Handbook of the Canadian Constitution*, 2017.
[40] *Thompson v. Canada (Deputy Minister of Agriculture)*, [1992] 1 S.C.R. 385 at 397-98.
[41] CSE, *Before the Beginning; the Examination Unit and the Joint Discrimination Unit*. www.cse-cst.gc.ca/en/about-apropos/history-histoire/before-avant; CSE, *The Beginning: The Communications Branch of the National Research Council*. www.cse-cst.gc.ca/en/about-apropos/history-histoire/beginning-histoire; and CSE, *Frequently Asked Questions*, www.cse-cst.gc.ca/en/about-apropos/faq.

affect an individual's constitutional rights.[42] Even apart from the Charter, the expanding scope of judicial review and Crown liability made courts increasingly unwilling to insulate government action from judicial scrutiny merely on the grounds that the authority is derived from the prerogative. For example, the Ontario Court of Appeal held that "the exercise of the prerogative will be justiciable, or amenable to the judicial process, if its subject matter affects the rights or legitimate expectations of an individual."[43] The Court referred to a "spectrum of reviewability," whereby matters of "high policy," such as the decision to sign treaties or go to war, remained largely beyond the purview of the courts, subject only to judicial review on Charter grounds.[44]

186. Nonetheless, while the Crown prerogative has been displaced or limited by Parliament or the courts, there are still areas in which the Crown prerogative is the only source of authority. These include powers relating to foreign affairs, such as declaring war and the making of treaties, and powers relating to the armed forces.[45] How the prerogative of defence is exercised has evolved over time to reflect principles of parliamentary accountability. As explained by professor Craig Forcese:

> In Canada's division of powers, the federal Parliament has exclusive authority over defence. Parliament has enacted the *National Defence Act* (NDA), which puts the [CAF] on a statutory footing. Constitutionally, the command of the military vests with the Governor General. However, in keeping with the constitutional conventions of responsible government, the Governor General does not decide when and where to deploy the CAF. In practice, this power is exercised by the federal Cabinet under the leadership of the Prime Minister.[46]

187. Forcese also describes at least two areas where Canadian law has limited, although possibly not wholly displaced, the prerogative as it relates to some DND/CAF functions. These include:

- **the deployment of the CAF pursuant to an executive order under the *Emergencies Act*:** Such a deployment would be subject to parliamentary scrutiny as a result of that statute's system of parliamentary review; and
- **the deployment of the CAF pursuant to subsection 273.6 (Public Service and Assistance to Law Enforcement) and Part VI (Aid of the Civil Power) of the *National Defence Act*:** These provisions

[42] Supreme Court of Canada, *Operation Dismantle Inc. v. R.*, [1985] 1 S.C.R. 441, [1985] S.C.J. No. 22, at para. 47 ["Operation Dismantle"]. And, *Canada (Prime Minister) v. Khadr*, 2010 SCC 3, where in 2010 the Supreme Court held that the Canadian government's failure to advance Omar Khadr's rights to American authorities was reviewable because it affected an individual citizen's constitutionalized rights. DND/CAF highlighted that the *Khadr* decision stated, "the review of an exercise of a prerogative power for constitutionality must remain sensitive to the fact that the executive branch is responsible for decisions made under this power, and the executive is better placed to make such decisions within a range of constitutional options." DND, Written submission to NSICOP, November 19, 2018.

[43] *Black v. Chretien* (2001), 199 D.L.R. (4th) 228 at para. 51.

[44] *Black v. Chretien* (2001), 199 D.L.R. (4th) 228, at para. 52. It has been noted that the Court of Appeal's discussion of the spectrum of reviewability and the concept of matters of "high policy" are *obiter* (an observation by a judge on a matter not specifically before the court or not necessary in determining the issue before the court), and rely on a single (English) authority: *R v. Secretary of State for Foreign & Commonwealth Affairs* (1988), [1989] 1 All E.R. 655 (Eng. C.A.). Nevertheless the Court of Appeal's *obiter* comments in *Black* have been followed in a number of subsequent cases. For example, in *Aleksic v. Canada (Attorney General)* (2002), 215 D.L.R. (4th) 720 (Ont. Div. Ct.) at 732; *Blanco v. Canada* (2003), 231 F.T.R. 3 at 6; *Turp v. Canada* (2003), 111 C.R.R. (2d) 184 (F.C.) at 188.

[45] Peter W. Hogg, Patrick H. Monahan, and Wade K Wright, *Liability of the Crown*, 4th ed., Carswell, 2011, at 1.5(b).

[46] Craig Forcese, "The Executive, the Royal Prerogative and the Constitution," in Peter Oliver, Patrick Macklem, and Nathalie Des Rosiers, eds., *The Oxford Handbook of the Canadian Constitution*, 2017.

of the Act have limited though not wholly replaced two analogous federal orders in council (which are themselves instances of the exercise of the Crown prerogative): the *Canadian Forces Assistance to Provincial Police Forces Directions*, which established a federal system of approving CAF assistance to provincial law enforcement agencies; and the *Canadian Forces Armed Assistance Directions*, which is the means by which the Commissioner of the RCMP or the Minister of Public Safety can request the assistance of the CAF's elite Special Forces and anti-terrorism unit (JTF2).[47]

188. Notwithstanding the evolution of the Crown prerogative, specifically that many of the Crown's immunities and privileges have been narrowed or eliminated by statute and the courts, including in the area of defence, neither the *National Defence Act* nor any other statute works to limit or displace the Crown prerogative to deploy the CAF on international missions. The Crown prerogative remains the source of authority for these deployments.[48]

The exercise of the Crown prerogative

189. Four primary actors can exercise the Crown prerogative to employ the CAF. According to the Office of the Judge Advocate General, these are: Cabinet, the Prime Minister, the Minister of National Defence, acting independently, or with the concurrence of the Minister of Foreign Affairs. Each of these actors has exercised the Crown prerogative that resulted in the use of defence intelligence activities in the course of a CAF operation.[49]

The Crown prerogative and defence intelligence

190. DND/CAF relies on the Crown prerogative as the authority for the conduct of defence intelligence activities and has stated that "the Crown prerogative is an efficient, effective and adaptable source of legal authority for military operations and defence activities that provides government with the ability to recognize and respond to crises around the world quickly and flexibly."[50] It has stated that the authority to conduct defence intelligence is implicit when the CAF is legally mandated, pursuant to legislation or an exercise of the Crown prerogative, to conduct military operations and other defence activities.[51] This means that defence intelligence activities may be authorized in the context of CAF deployments. The Defence Policy states, "Intelligence is Canada's first line of defence. The defence of Canada, the ability to operate effectively overseas, and the capacity to engage internationally are

[47] Craig Forcese, *The Executive, the Royal Prerogative and the Constitution*, in Peter Oliver, Patrick Macklem, and Nathalie Des Rosiers, eds., *The Oxford Handbook of the Canadian Constitution*, 2017.
[48] Office of the Judge Advocate General, *The Crown Prerogative in Canada as applied to Military Operations*, Strategic Legal Paper Series, Issue 2, 2008; and Craig Forcese, *The Executive, the Royal Prerogative and the Constitution*, in Peter Oliver, Patrick Macklem, and Nathalie Des Rosiers, eds., *The Oxford Handbook of the Canadian Constitution*, 2017.
[49] Office of the Judge Advocate General, *The Crown Prerogative in Canada as applied to Military Operations*, Strategic Legal Paper Series, Issue 2, 2008.
[50] Department of National Defence. Written submission to NSICOP, November 19, 2018.
[51] DND, ***, April 27, 2018.

heavily dependent on the systematic collection, coordination, fusion, production and dissemination of defence intelligence."[52] DND/CAF has also stated that ***."[53]

191. The Committee was briefed on two notable examples where DND/CAF, under the authority of the Crown prerogative, developed a new defence intelligence activity or created a new domain of military operations. In the case of intelligence activities, DND/CAF stated that its CAF HUMINT capability had evolved as an operational area of defence intelligence since the Canadian ***.[54] When the Minister of National Defence authorized the creation *** for use in ***, he did so under the authority of the Crown prerogative, and consistent with the DND/CAF's internal administrative obligation that each *** of HUMINT capabilities be approved by the Minister.[55]

192. With respect to domains of military operations, DND/CAF stated that in 2015 it received Government approval to develop new capabilities for active cyber operations, to be conducted in accordance with Government direction. DND/CAF described this as the development of a new domain of military operations, analogous to the air, land, or sea domains, and that the "***."[56] DND officials noted that they sought Government approval because of the requirement for new resources, and because those new capabilities could affect the interests of other organizations, namely Global Affairs Canada (foreign policy considerations) and CSE (existing cyber technical and operational expertise).[57]

193. DND/CAF stated that the conduct of defence intelligence activities under the Crown prerogative is subject to the requirement for a "nexus," or a "reasonable connection," between defence intelligence activities and a defence mission. [*** Information in paragraphs 193, 194 and 195 has been removed in its entirety.***]

***[58]

194. ***[59]

195. Questions regarding the Crown prerogative and defence intelligence have persisted. ***[60]

***

***[61]

[52] "Enhancing Defence Intelligence," Canada's Defence Policy – *Strong, Secure, Engaged*, pp. 65–66, accessed at: dgpapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf.
[53] DND, ***, April 27, 2018.
[54] DND, Information briefing to the NSICOP Secretariat, August 3, 2018.
[55] DND, Written submission to NSICOP, July 4, 2018.
[56] DND, "***," April 27, 2018; and DND, Written submission to NSICOP, November 19, 2018.
[57] DND, Information briefing to NSICOP Secretariat, August 3, 2018.
[58] DND, ***, July 18, 2003.
[59] DND, ***, July 18, 2003.
[60] Department of Justice, ***, June 15, 2012.
[61] Department of Justice, ***, June 15, 2012.

196. In 2013, DND/CAF formalized the requirement for a nexus in the Ministerial Directive on Defence Intelligence, which states, "There [must] be a clear nexus between the nature and scope of the defence intelligence activity and DND/CF's mandated defence operations or activities."[62] In explaining the meaning of the nexus requirement, DND/CAF officials stated that the deployment and use of a particular intelligence activity must have a clear connection to the objectives of the mission. DND/CAF also stated that the requirement for a clear nexus between a defence intelligence activity and the legally mandated mission serves as "a constraint on defence intelligence activities."[63]

197. DND/CAF responded to questions from the Committee on how nexus is determined and how the resulting constraint works in practice. DND/CAF stated that there is no statutory requirement for a nexus between a defence intelligence activity and a legally-mandated mission: it is a policy requirement found in the Ministerial Directive on Defence Intelligence. DND/CAF described nexus as "a term of art," and noted that it does not have a standard guideline or standardized process for determining a nexus.[64] Rather, DND/CAF stated that the process of defining a nexus begins with the Government's authorization of a mission, which serves as a "macro-nexus" for defence intelligence activities.[65]

198. Nexus is then refined through the operational planning process, a formal procedure to assess mission requirements for forces and assets, including defence intelligence capabilities. As part of this process, DND/CAF considers issues like the threat facing CAF personnel, the availability of intelligence personnel and equipment, and the commander's assessment of mission needs and where Canadian personnel could contribute to coalition objectives. These assessments are subject to rigorous legal and policy review to ensure that the use of defence intelligence activities is linked, in each case, to the legally authorized mandate of the mission. DND/CAF stated that the planning process is "synonymous with the determination of nexus"[66] and that nexus is defined on a case-by-case basis to ensure maximum flexibility for commanders. Any constraints identified in this process, and under a specific nexus, are codified through the chain of command and operational orders, which impose a lawful requirement on CAF personnel to adhere to those constraints.[67] NSICOP asked if there was an element of proportionality in the determination of a nexus – to which DND/CAF stated that it does not view nexus as a *proportional* constraint on defence intelligence activities; rather, that it functions as a means to customize intelligence-gathering activities to the needs and legal mandate of each mission.[68]

[62] DND, Ministerial Directive on Defence Intelligence, undated, signed by the Honourable Rob Nicholson, Minister of National Defence.
[63] DND, Written submission to NSICOP, November 19, 2018.
[64] DND, Oral testimony to NSICOP, December 4, 2018.
[65] DND, Oral and written submissions to NSICOP, November 1, 2018, and November 19, 2018.
[66] DND, Written submission to NSICOP, November 19, 2018.
[67] DND/CAF asserts that the CAF chain of command, established in the *National Defence Act*, means that when orders are given to implement policy, this gives the policy the weight of law: "The military chain of command ensures that [CAF] is subject to well-defined checks and balances through military command and control, the governance framework established by CFINTCOM and CDI, and the operation of relevant domestic and international law." DND, Written submission to NSICOP, November 26, 2018.
[68] DND, Written submission to NSICOP, November 19, 2018; and DND, Oral testimony to NSICOP, December 4, 2018.

NSICOP assessment of nexus

199. The Committee believes it is important that the conduct of defence intelligence activities be governed by a comprehensive authority framework. It has observed that components of this framework are already in place. For example, DND/CAF SIGINT activities run the risk of intercepting private communications. These risks are mitigated through the Ministerial Directive on the Integrated SIGINT Operations Model, which establishes the framework whereby the CAF conducts foreign intelligence activities under CSE authorities, subject to the same limitations imposed on CSE through the *National Defence Act*. Components of the framework also exist in the area of CAF HUMINT operations: for example, conducting interrogations of detainees could entail risks of running afoul of domestic or international legal standards. DND/CAF has mitigated these risks in several ways: for example, the conduct of HUMINT activities must be authorized by the Minister in each case and HUMINT operations are subject to oversight at multiple levels. In the same vein, the requirement for a nexus between the authority of the mission and the activities undertaken in support of it is meant to address the risks identified *** concerning the collection of intelligence beyond what is necessary.

200. The Committee spent considerable time trying to understand the meaning of nexus and how it is determined. Beyond the notion that nexus means a reasonable connection between a legally mandated mission and the defence intelligence activity undertaken in support of it, NSICOP is not convinced that the authority framework provides sufficient guidance to determine the connection. DND/CAF acknowledged it does not have a standard process or test for determining it.

201. That said, NSICOP fully agrees that the requirement for a nexus is important and should function as a constraint on defence intelligence activities. In its view, however, the determination of a nexus can only function as a constraint on defence intelligence activities if it is defined according to clear principles. NSICOP offers two principles that are well-established in law and could be adapted to the unique circumstances of DND/CAF. The first is 'reasonableness' – how should DND/CAF officials determine whether the use of a specific defence intelligence capability is 'reasonable' in the context of a legally mandated mission? The second is 'proportionality' – how should DND/CAF officials determine which defence intelligence activities are proportional to the objectives of the mission? Given the importance of the identification of a nexus as one of two conditions that must be met before using defence intelligence activities (see paragraph 208), the development of standard guidelines for determining nexus would fill a significant gap, help ensure consistency in decision-making and enhance the transparency of the process.

Governance and oversight of defence intelligence

202. This section describes the mechanisms DND/CAF has put in place to ensure the governance and accountability of its defence intelligence activities, and the internal review and oversight of those activities.

203. As discussed in Chapter 3 on intelligence priorities, the processes that are put in place to govern intelligence activities are fundamental to ensuring accountability over intelligence activities and operations. In the context of the Crown prerogative, DND/CAF has developed an internal governance structure and administrative system to address risks in the collection of intelligence and to ensure accountability. Such a system is important. ***[69] The Ministerial Directive on Defence Intelligence makes the same point:

> It is imperative that the governance and accountability of defence intelligence activity keep pace with the ongoing evolution of intelligence activity and of [Government of Canada] security and intelligence community standards.[70]

204. The administrative system consists of five primary mechanisms through which direction and guidance is given for the conduct of defence intelligence activities. These mechanisms have been used to establish several governance bodies to provide oversight and accountability of defence intelligence activities. These mechanisms include:

- **Ministerial Directive on Defence Intelligence:** This directive sets the principal value of intelligence to national defence, national security, and foreign affairs; outlines the authorities for defence intelligence activities; and provides a strategic framework for policy and legal authorities for defence intelligence.[71]
- **Ministerial Directive on Defence Intelligence Priorities:** This directive is based on the biannual process of setting the Government of Canada intelligence priorities and provides direction to the Deputy Minister and Chief of the Defence Staff to focus defence intelligence collection, analysis, production, and assessment on specific issues.[72]
- **Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities:** This direction prohibits the disclosure or requesting of information that would result in a substantial risk of mistreatment of an individual by a foreign entity, and certain uses of information that was likely obtained through the mistreatment of an individual by a foreign entity.[73]
- **Ministerial authorizations:** These are sought to conduct sensitive defence intelligence activities, including HUMINT and SIGINT activities.[74]

[69] DND, ***," January 28, 2014.
[70] DND, Ministerial Directive on Defence Intelligence, undated.
[71] DND, Assistant Chief of Defence Intelligence, Speaking points, Written submission to NSICOP, June 19, 2018; and DND, Ministerial Directive on Defence Intelligence, undated.
[72] Canadian Forces Intelligence Command, *2016 Annual Report on Defence Intelligence to the Minister of National Defence.*
[73] DND, Ministerial Direction to the Department of National Defence and the Canadian Armed Forces: Avoiding Complicity in Mistreatment by Foreign Entities, October 12, 2017.
[74] DND, Speaking points of the Assistant Chief of Defence Intelligence, given to the NISCOP Committee, June 19, 2018. See paragraphs 180 and 181.

- **CDI functional directives:** The CDI provides functional direction to the Defence Intelligence Program to ensure that defence intelligence activities are carried out in a responsive, efficient, and accountable manner. To date, 26 functional directives have been issued pertaining to the oversight, conduct, development, and employment of defence intelligence capabilities and activities, spanning all of the capability areas of the Program.

205. The Committee recognizes the importance of each of these mechanisms. For the purposes of this review, however, it will focus on the Ministerial Directive on Defence Intelligence for its foundational role in the development, use, and oversight of defence intelligence capabilities. (The importance of the Ministerial Directive on Defence Intelligence Priorities is also discussed as part of the Committee's review of the Government's intelligence priorities in Chapter 3, and functional directives from the CDI are referenced below, as required.)

The Ministerial Directive on Defence Intelligence

206. The Ministerial Directive on Defence Intelligence (hereafter, the Ministerial Directive) establishes the accountability of the Minister, in authorizing defence intelligence activities, to Parliament and as a Minister of the Crown. The Ministerial Directive also establishes the accountability of DND and CAF officials to the Minister in the conduct and oversight of defence intelligence activities.

207. The Ministerial Directive states that DND/CAF may develop, generate, and employ such intelligence capabilities as are required to enable lawful, timely, and effective decisions.[75] Such decisions would support the core roles and missions of the CAF, including: the defence of Canada; the defence of North America (with the United States); the promotion of international peace and security; CAF capability development, including research and development and defence procurement; and lawful requests from other government departments for defence intelligence support.

[75] Joint Doctrine Branch Canadian Forces Warfare Centre, *Canadian Forces Joint Publication (CFJP) 2.1 Intelligence Operations*, August 2017. Force generation is defined in departmental documentation as the process of organizing, training and equipping forces for the application of military means in support of strategic objectives, and the command, control, and sustainment of allocated forces.

208. The Ministerial Directive states that the authorities, mandate, and mission in regard to defence intelligence are tied to two principles:

- there must be a clear nexus between the nature and scope of the defence intelligence activity conducted and the legally mandated defence operations or activities; and
- where lawfully requested, the activity must comply with the mandate and authority of the requesting body.

209. The Ministerial Directive provides clear direction on the line of accountability to the Minister regarding defence intelligence, and includes both the Chief of the Defence Staff and the Deputy Minister of National Defence. The Chief of the Defence Staff is accountable to the Minister for the generation of CAF capabilities, specifically including defence intelligence capabilities. This includes oversight and control of defence intelligence activities. The Deputy Minister is accountable for the provision of policy advice in all defence intelligence matters, including the alignment of defence intelligence activities with wider Government policies and initiatives and on matters of international defence relations. The Ministerial Directive also directs the Deputy Minister and the Chief of the Defence Staff to work collaboratively across their respective areas of responsibility and accountability to "ensure that appropriate policies, directives and oversight structures are developed and implemented to maintain the maximum possible responsiveness, effectiveness and accountability of defence intelligence."

210. The Ministerial Directive obligates the Deputy Minister and the Chief of the Defence Staff to keep the Minister informed of defence intelligence activities in accordance with the Minister's mandate and responsibilities. The Ministerial Directive states that the Deputy Minister and the Chief of the Defence Staff must conduct "appropriate interdepartmental and legal consultations" before authorizing or initiating any defence intelligence activity they consider sensitive or that may involve:

- national security or sovereignty;
- any serious threat to the lives and/or legal or constitutional rights of persons in Canada and Canadian citizens around the world, or to the rights of individuals more broadly as recognized by international law;
- any serious threat to the protection and/or advancement of Canada's foreign relations and reputation abroad;
- any potential risk of exposure, real or perceived, of the [Government of Canada], DND or [the CAF] to any significant domestic or international legal liability, or to circumstances that would contravene the DND/CF Code of Values and Ethics; and
- all matters or activities that may entail significant financial commitments outside of Government of Canada investments and expenditures.

211. The Committee sought additional information from DND/CAF, on three key areas of the Ministerial Directive:

- **Ministerial responsibilities and accountability:** through what means, and how often, has DND/CAF advised the Minister of the use or development of defence intelligence capabilities or arrangements that may be sensitive and engage the risks outlined in the Ministerial Directive?
- **Determining the sensitivity of defence intelligence activities:** how does DND/CAF measure or evaluate the sensitivity of specific defence intelligence activities or arrangements?

- **Interdepartmental and legal consultations:** what degree of interdepartmental and legal consultation takes place regarding the use and development of defence intelligence capabilities? How does DND/CAF mitigate risks or concerns raised in those consultations?

212. The Committee considers each of these areas below.

Ministerial responsibilities and accountability

213. As outlined above, the Ministerial Directive provides direction to the Deputy Minister and the Chief of the Defence Staff across a range of areas related to defence intelligence activities, and on their obligations to the Minister. The governance of defence intelligence is a key area, as it constitutes a critical element of the accountability framework for the Minister and his or her officials for defence intelligence activities.[76]

214. The Minister of National Defence included in the Ministerial Directive an obligation for the Deputy Minister and the Chief of the Defence Staff to report annually on "defence intelligence governance, performance, strategic priorities, major program and special project initiatives, and any policy, legal and management issues of significance." The Ministerial Directive also indicates that the Commander, Canadian Forces Intelligence Command (that is, the CDI) is accountable to the Deputy Minister and the Chief of the Defence Staff for producing scheduled and ad hoc reports on compliance with functional direction. To date, DND/CAF has produced annual reports to the Minister of National Defence on the defence intelligence program for the years 2015, 2016, and 2017.

Annual Reporting on governance, performance, and priorities

215. The *2015 Annual Report on Defence Intelligence to the Minister of National Defence* identified the Defence Intelligence Management Committee (DIMC), chaired by the CDI, as the principal internal governance entity enabling the CDI to provide coordinated strategic direction and oversight of defence intelligence and through which issues concerning strategic direction, oversight, and compliance may be brought forward to the Deputy Minister and Chief of the Defence Staff for consideration.[77] The DIMC's role in enabling the CDI to provide strategic direction and oversight of defence intelligence is also referenced in the 2016 and 2017 annual reports.[78] The DIMC terms of reference and DND/CAF documentation on the defence intelligence governance structure indicate the DIMC is also meant to consider proposals or plans for intelligence capabilities or relationships that are sensitive, or the use or employment of sensitive intelligence collection capabilities and relationships, and to brief the Deputy Minister or the Chief of the Defence Staff when contemplating, or seeking approval for, the development and use of sensitive defence intelligence capabilities and activities.[79]

[76] Canadian Forces Intelligence Command, *2015 Annual Report on Defence Intelligence to the Minister of National Defence.*
[77] Canadian Forces Intelligence Command, *2015 Annual Report on Defence Intelligence to the Minister of National Defence.*
[78] Canadian Forces Intelligence Command, *2016 Annual Report on Defence Intelligence to the Minister of National Defence* and *2017 Annual Report on Defence Intelligence to the Minister of National Defence.*
[79] DND, *Defence Intelligence Governance Structure*, April 27, 2018; and DND, written response to follow-up questions pertaining to the Ministerial Directive on Defence Intelligence, July 4, 2018.

216. DND/CAF has acknowledged that the DIMC did not work as fully intended.[80] In the course of the review, DND/CAF demonstrated that the Minister of National Defence is consulted on and approves the use of specific sensitive defence intelligence capabilities. However, these consultations did not arise as a result of work done at the DIMC, because, as DND/CAF stated, it was more suited to dealing with the management of the defence intelligence enterprise, such as policy development, priority setting, and human resources matters. It also suffered from an overly broad membership and met too infrequently (not more than quarterly) to fulfill its intended role. Instead, DND/CAF brought defence intelligence matters considered to be sensitive directly to the Deputy Minister, the Chief of the Defence Staff, or the Minister for consideration or decision.[81]

217. DND/CAF also informed the Committee that it has had no program to measure compliance with the Ministerial Directive and has done limited formal measurement of compliance, but that it exercises oversight and compliance through the chain of command and with discipline-specific oversight bodies for particularly sensitive intelligence activities (outlined in paragraph 221, below). DND/CAF stated that two new internal bodies are being established to provide centralized oversight of defence intelligence activities: the Directorate of Intelligence Review, Compliance and Disclosure, which will establish a formal program of compliance for the entire defence intelligence program; and the Defence Intelligence Oversight Board, which will be chaired by the Deputy Minister and the Chief of the Defence Staff, will convene three times per year, and will report to the Minister through a dedicated section of the Annual Report on Defence Intelligence to the Minister of National Defence.[82] The annual reports on defence intelligence did not raise the fact that the DIMC did not fulfill its intended role, nor that this posed potential challenges for the oversight of defence intelligence activities.

NSICOP assessment

218. Consistent with obligations for annual reporting in the Ministerial Directive, DND/CAF has provided annual reports on defence intelligence to the Minister of National Defence since 2015. As noted in paragraph 210, each report must inform the Minister of significant issues related to governance, performance, strategic priorities, major program and special project initiatives, and policy, legal, and management issues pertaining to defence intelligence. In the Committee's view, the fact that the DIMC did not "undertake a key role in monitoring compliance and communicating sensitive issues to senior decision-makers"[83] is a governance and management issue of significance, one that DND/CAF is now addressing through the creation of two separate bodies. The annual reports do not address other important obligations in the Ministerial Directive, such as legal or interdepartmental consultations that have been undertaken due to the magnitude of risks to Canada's foreign relations or reputation, or threats to the rights of Canadian citizens, which may have arisen as a result of the authorization or initiation of defence intelligence activities or relationships. The Committee believes that including

[80] DND, *Defence Intelligence Governance Structure*, April 27, 2018; and DND, Written submission to NSICOP, July 4, 2018. DND/CAF stated that, "It was intended, at one point, that the DIMC undertake a key role in monitoring compliance and communicating sensitive issues to senior decision-makers."

[81] DND, written submission to NSICOP, July 4, 2018.

[82] DND, Written submission to NSICOP, July 4, 2018; and Oral testimony to NSICOP, December 4, 2018.

[83] DND, Written submission to NSICOP, July 4, 2018.

elements such as these in future annual reports would enhance the Minister's accountability for defence intelligence activities.

219. Though these bodies are in their early stages, the Committee believes that the establishment of the Directorate of Intelligence Review, Compliance and Disclosure, and the Defence Intelligence Oversight Board should enhance DND/CAF's tracking and measurement of compliance, and will support the Minister in his accountability for the defence intelligence program.

Determining the sensitivity of defence intelligence activities

220. The Ministerial Directive includes specific requirements with respect to sensitive issues. As outlined in paragraph 209, the Ministerial Directive obligates the Deputy Minister and the Chief of the Defence Staff to engage in interdepartmental and legal consultations before authorizing or initiating any defence intelligence activity they consider to be sensitive, or that may impact Canada's national security or sovereignty, threaten the lives and constitutional rights of persons in Canada and Canadian citizens around the world, or threaten Canada's foreign relations and reputation abroad.

221. DND/CAF described its understanding and definition of "sensitive" in relation to defence intelligence capabilities as "requiring special protection from disclosure that could cause embarrassment, [or] threaten or compromise security."[84] Each defence intelligence activity area considered to be sensitive has an identified internal oversight body, prescribed consultations and varying reporting requirements, as listed in Table 3.

Sensitive Activity Area	Oversight Body	Consultations With	Reporting to Senior Officials and the Minister
HUMINT	Chief of the Defence Staff HUMINT Authorization Board	CSIS, Judge Advocate General / Canadian Forces Legal Advisor	Annual Report to the Chief of the Defence Staff on *** Reviews by contractor
***	*** Evaluation Review Board	Global Affairs Canada; CSIS; CSE; Canada Border Services Agency; Immigration, Refugees and Citizenship Canada; Judge Advocate General / Canadian Forces Legal Advisor	Annual Report to the Minister and the Treasury Board of Canada Secretariat

[84] DND, Written submission to NSICOP, May 23, 2018.

Sensitive Activity Area	Oversight Body	Consultations With	Reporting to Senior Officials and the Minister
Counter-Intelligence	Counter-Intelligence Oversight Committee	CSIS, RCMP, Judge Advocate General / Canadian Forces Legal Advisor, and other law enforcement / security agencies as applicable	No reporting requirement
SIGINT	Commander, Canadian Forces Information Operations Group (with CSE compliance team)	CSE, Judge Advocate General / Canadian Forces Legal Advisor	Specific annual reports from the Office of the CSE Commissioner
***	Commander, Canadian Forces Intelligence Command	CSIS, CSE, Judge Advocate General / Canadian Forces Legal Advisor	No reporting requirement

Table 3. DND/CAF Oversight Matrix of Sensitive Defence Intelligence Capabilities

Governance of human intelligence (HUMINT)

222. This section details one of the sensitive defence intelligence activity areas for which ministerial authorizations are required to enable their use ***: HUMINT *** activities.

223. All HUMINT personnel for operations *** must be approved by the Minister of National Defence. All HUMINT activities are subject to formal oversight by the Chief of the Defence Staff HUMINT Authorization Board, chaired by the Chief of the Defence Staff. The Board convenes annually to review the overall conduct of HUMINT operations (***). The Board includes representation from across the defence intelligence program, the Judge Advocate General, and CSIS.[85] Annual reports on *** operations are produced for the Chief of the Defence Staff, who briefs the Minister, and the HUMINT program is subject to regular staff assistance visits to ensure the activities comply with policy and direction.[86]

224. Guidance and direction for HUMINT *** operations come from CDI functional directives, such as CDI Functional Directive: CF Policy Framework for the Conduct of HUMINT Activities. Among other things, this CDI directive stipulates that ministerial authorization is required for [*** This text lists conditions imposed by the directive.***]; and that the Minister or the Chief of the Defence Staff may order an external review of such operations.[87]

[85] CSIS representation on the Board is due to its mandate, role, and expertise related to HUMINT operations, and the need for de-confliction between DND/CAF and CSIS, where both may conduct HUMINT activities ***.
[86] DND, written submission to NSICOP, July 4, 2018.
[87] DND, CDI Functional Directive: CF Policy Framework for the Conduct of HUMINT Activities.

225. In the case of HUMINT *** operations ***, the ministerial authorization directed the Chief of the Defence Staff to "conduct *** human intelligence (HUMINT) operations in support of ***." The Minister also directed that, "an External Review *** be conducted and a classified report prepared for the [Minister] annually, to provide assurance of [CAF] compliance with the [Minister's] Letter of Approval and associated directives issued by the chain of command."[88]

226. In accordance with the Minister's direction, three external reviews of HUMINT *** operations *** were conducted by an external contractor ***. The contractor identified specific issues, including instances of non-compliance with senior-level direction, and errors, omissions, and ambiguities in the official documentation recording chain of command decisions. Recommendations were made to improve reporting to the Minister of National Defence, and to improve rigour, quality control, and review and oversight ***. The reviews also recommended that the CDI directive on CF HUMINT *** be revised to mitigate "divergent interpretations of [the CDI Directive . . . which] contributed to instances of non-compliance."[89] DND/CAF accepted the recommendations and revised the functional directive.

227. The CAF did not conduct HUMINT activities in operations between ***. ***, the Minister authorized HUMINT *** operations *** late that year. [*** The following text describes an order by the Chief of the Defence Staff to conduct a review of HUMINT operations, and that DND/CAF did not do so in any of the following three years.***].[90] ***.[91]

[88] DND, Canadian Forces Intelligence Command, *Summary of External Reviews into CF HUMINT ****, April 27, 2018; and DND, *Report to the Minister of National Defence. External Review. ****. The CDI functional directive that details HUMINT *** is the *Chief of Defence Intelligence Functional Directive: CF HUMINT ****.

[89] DND, Report to the Minister of National Defence. External Review. ***.

[90] DND, Chief of the Defence Staff, CDS Directive 002 ***.

[91] DND, Chief of the Defence Staff HUMINT Authorization Board 23 November 2017 – Minutes, December 13, 2017.

Internal evaluations of defence intelligence activities

228. Since 2001, defence intelligence activities have been subject to three internal evaluations:

Date	Review	Review Body	Type
2002	Internal Evaluation of Defence Intelligence	DND Review Services	Internal
2004	Defence Intelligence Review (DIR)	DND-wide	Internal
2015	Internal Evaluation of Defence Intelligence	DND Review Services	Internal

Table 4. Internal Evaluations of Defence Intelligence Activities

229. The 2015 internal evaluation of defence intelligence was conducted by DND/CAF's Review Services group and covered the 2009–2014 period. The internal review focused on an examination of immediate outcomes, intelligence activities, governance, and coordination among the elements of the defence intelligence organization at that time. It assessed that there was an ongoing and demonstrable need for defence intelligence, and that the defence intelligence program remained relevant in an evolving threat environment by producing actionable defence intelligence for DND/CAF and the Government of Canada, and as a key enabler of military operations. The evaluation also noted areas for improvement. These included the governance of the defence intelligence program, including consolidating and generating governance documentation; updating CAF doctrine and clarifying CDI roles and responsibilities; and developing new human resources strategies for defence intelligence (particularly for civilian analysts). The 2015 evaluation concluded that defence intelligence was well-aligned with government roles, responsibilities, and priorities, and the conduct of defence intelligence activities was appropriate for supporting the Government's right to self-defence.[92]

230. DND/CAF also conducted audits and reviews of specific defence intelligence activities. The first was a two-phase internal audit of the *** by DND Review Services in 2013–2014. Operated by the Canadian Forces Intelligence Command, *** assesses the threat posed by ***.[93] The second was the aforementioned external reviews of the CAF's HUMINT *** operations ***, to ensure that the operations complied with all policies and directives.

NSICOP Assessment

231. DND/CAF has addressed recommendations from its internal evaluations, audits, and reviews. For example, it created the position of Chief of Defence Intelligence in December 2005 to respond to the 2004 Defence Intelligence Review, and established the CDI as the functional authority for the defence intelligence program in 2013 with the creation of the Canadian Forces Intelligence Command. It continued to expand and update its governance documentation and implemented a human resources

[92] DND, Assistant Deputy Minister (Review Services), Evaluation of Defence Intelligence, November 2015.
[93] DND, Assistant Deputy Minister (Review Services), summary note regarding the internal audit of the ***.

strategy in 2016 for the recruitment and career development of defence intelligence analysts to respond to the 2015 review.[94]

232. In its briefings to the Committee and as articulated in the Defence Policy, DND/CAF acknowledged the importance of civilian review of national security and intelligence activities.[95] However, neither NSICOP nor NSIRA (in its proposed legislation) has a statutory *obligation* to conduct regular reviews of DND/CAF defence intelligence activities. As a result, gaps in ongoing, external review will remain; risks arising from the absence of external review can only be said to be partially mitigated.

Interdepartmental and legal consultations

233. The Ministerial Directive requires officials to conduct interdepartmental and legal consultations prior to authorizing and initiating sensitive defence intelligence activities. DND/CAF stated that consultations with their legal services take place at all levels as a matter of practice, and noted that, "Interdepartmental consultations take place where [defence intelligence] activities impact the mandate of other government departments and agencies, or vice versa."[96]

234. DND/CAF provided an illustrative list of specific issues and activities on which it consulted legal counsel and other government departments within the last two years. These included:

- HUMINT activities – consulted the Judge Advocate General and Canadian Forces Legal Advisor and CSIS;
- SIGINT activities – consulted the Judge Advocate General and Canadian Forces Legal Advisor and CSE;
- Counter-Intelligence activities – consulted the Judge Advocate General and Canadian Forces Legal Advisor, CSIS, and the RCMP;
- *** activities – consulted the Judge Advocate General and Canadian Forces Legal Advisor, Global Affairs Canada, CSIS, CSE, the Canada Border Services Agency, and Immigration, Refugees and Citizenship Canada;
- Policy governing *** – consulted the Judge Advocate General and Canadian Forces Legal Advisor, CSIS, and CSE; and
- Implementation of the Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities – consulted the Judge Advocate General and Canadian Forces Legal Advisor, Global Affairs Canada, CSIS, the RCMP, and CSE.[97]

235. The Committee asked DND/CAF to provide specific examples of consultations with other government departments, consistent with the Ministerial Directive's requirement. DND/CAF provided one example, below, which raised systemic issues related to the procedure DND/CAF uses for

[94] DND, Canadian Forces Intelligence Command, Briefing Note (with annexes) regarding the career management of the Canadian Forces Intelligence Command's Civilian Intelligence Cadre, March 26, 2018.
[95] "Enhancing Defence Intelligence," *Canada's Defence Policy – Strong, Secure, Engaged*, pp. 65–66, accessed at: http://dgpapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf; and DND, remarks of the Chief of the Defence Staff and the Deputy Minister to NSICOP during DND site visit and information briefing, March 20, 2018.
[96] DND, written response to follow-up questions pertaining to the Ministerial Directive on Defence Intelligence, July 4, 2018.
[97] DND, written submission to follow-up questions pertaining to the Ministerial Directive on Defence Intelligence, July 4, 2018.

interdepartmental consultation, notably that DND/CAF does not have a standard process to engage other departments with regard to defence intelligence activities as part of the planning and execution of deployed operations.[98]

236. [*** Paragraphs 236, 237 and 238 were revised to remove information that may be injurious and to ensure readability. The paragraphs describe an example where DND/CAF informed the Minister of National Defence that it would consult Global Affairs Canada, consistent with the 2013 Ministerial Directive on Defence Intelligence. The Ministerial Directive states, "the CDS and/or the DM must undertake appropriate interdepartmental and legal consultations before authorizing or initiating any defence intelligence activity that they consider to be particularly sensitive, or that is likely to present a significant impact on any of the following areas: ....any serious threat to the protection and/or advancement of Canada's foreign relations and reputation abroad..." Neither DND/CAF nor Global Affairs Canada could provide the Committee a record of that consultation. DND/CAF stated that it had no standard process for interdepartmental consultations in such cases, but that the consultations happen informally on a day-to-day basis at the staff level. Global Affairs Canada stated that, had it been consulted, it would have conducted assessments in certain areas, including of implications for Canada's foreign relations.***].[99] ***.[100]

237. ***.[101] ***.[102]

238. ***.[103] ***.[104] ***.[105]

NSICOP assessment

239. [*** This paragraph was revised to remove information that may be injurious and to ensure readability. The paragraph describes the Committee's assessment of one of two issues of importance. The first is that DND/CAF made its own determination of the foreign relations risks associated with an activity. Global Affairs Canada is the organization responsible for assessing those risks. While DND/CAF asserted that consultations with Global Affairs Canada are routine and institutionalized, it did not provide evidence in this example that it consulted the department, contrary to the requirements of the

[98] DND, "Response to [request for information] on consultations with [other government departments]," Written submission to NSICOP, September 12, 2018.
[99] DND, Written submission to NSICOP, July 4, 2018; DND, ***; and DND, written submission to NSICOP, November 19, 2018.
[100] DND, ***.
[101] The first requirement was noted in a written response to follow-up questions pertaining to the Ministerial Directive on Defence Intelligence. DND, Written submission to NSICOP, July 4, 2018. As discussed in paragraph 210 of this report, the second requirement is stipulated in the Ministerial Directive on Defence Intelligence.
[102] DND, ***.
[103] DND, Email, "Response to [request for information] on consultations with [other government departments]," September 12, 2018. *** Global Affairs Canada, "Follow-up re: DND Consultation," Written submission to NSICOP, November 2, 2018.
[104] DND, "FW: NSICOP – clarification on consultation with OGDs," Written submission to NSICOP, October 22, 2018.
[105] NSICOP Secretariat meeting with Global Affairs Canada, August 7, 2018.

Ministerial Directive. As a result, Global Affairs Canada did not conduct its own assessment.***].[106] *** [107]

240. The second issue is the absence of a formal process for interdepartmental consultations on the use of defence intelligence activities in operations. The Committee is concerned that the absence of such a process, at least in this case, resulted in the inability of DND/CAF to produce a record of an interdepartmental consultation required by ministerial direction.

[106] DND, ***.

[107] DND, Information briefing to the NSICOP Secretariat, October 19, 2018; and DND, "FW: NSICOP – clarification on consultation with [other government departments]," Written submission to NSICOP, ***, October 22, 2018.

Defence intelligence: The question of legislation

241. As Parliamentarians, we have been struck throughout the course of our work by the different authority structures that govern Canada's security and intelligence organizations and how these authority structures have evolved over time. The Committee's decision to conduct a review of DND/CAF intelligence activities was driven in part by the need to understand the authorities under which those activities were conducted. Paragraphs 171 to 200 examined the authority framework for DND/CAF defence intelligence activities. NSICOP notes that the current framework does not include an act of Parliament, given that defence intelligence activities are grounded in the Crown prerogative. Consistent with the Committee's mandate to review Canada's legislative framework for national security and intelligence, the question that is posed is legitimate: should consideration be given to placing DND/CAF intelligence activities on a statutory footing?

242. This review has also given rise to questions of comparison, both domestically and internationally: where are the activities and authorities of different organizations similar and different, and why? As discussed in this chapter, DND/CAF, CSIS, and CSE all conduct similar intelligence activities, albeit under different mandates and authorities. CSIS and CSE were given statutory bases in 1984 and 2001, respectively. Legislation for both organizations was carefully constructed to account for very different mandates, operating environments, and operational risks. The Committee summarizes these changes below, and following that, considers the question of whether the Government should provide DND/CAF with an explicit statutory basis for the conduct of defence intelligence activities in support of military operations.

243. Internationally, other countries have considered the role of their parliaments or legislatures in approving or constraining military activities.[108] Most inquiries or studies in Commonwealth countries centered on the legislative displacement of the Crown prerogative with regard to decisions for the deployment of forces.[109] To NSICOP's knowledge, no detailed analysis has been conducted in relation to parliamentary roles in regard to defence intelligence activities. None of Canada's Five Eyes partners have legislated parliamentary (for Commonwealth members) or congressional (for the United States) roles in approving a government's decision to deploy armed forces abroad.[110] The United Kingdom has come closest, although its government is not legally required to receive parliamentary approval prior to the deployment of armed forces.[111] U.K. parliamentary committees have studied this issue at length since 2003 and proposed a number of means to formalize Parliament's role in legislation, though none of those efforts have closely examined the question of legislation for defence intelligence activities.

[108] Michael Dewing and Corinne McDonald, "International Deployment of Canadian Forces: Parliament's Role," PRB 00-06E, Parliamentary Information and Research Service, Library of Parliament, May 18, 2006; and Geneva Centre for the Democratic Control of Armed Forces (DCAF), *Parliamentary War Powers: A Survey of 25 European Parliaments*, Occasional Paper – No. 21.
[109] The question has been studied most extensively in the United Kingdom, regarding the role of Parliament in approving military action in the Iraq War and the Syrian Civil War. See, e.g., House of Lords, Constitution Committee, *Waging War: Parliament's Role and Responsibility*, 15th Report Session 2005–06, HL Paper 236; and House of Lords, Constitution Committee, *Constitutional Arrangements for the use of Armed Force*, 2nd Report Session 2013–14, HL Paper 46.
[110] Geneva Centre for the Democratic Control of Armed Forces (DCAF), *Parliamentary War Powers Around the World, 1989–2004. A New Dataset*, Occasional Paper – No. 22.
[111] For a detailed analysis of the United Kingdom's attempts at formalizing Parliament's role in the decision to deploy armed forces abroad since 2003, and the disagreements that persist in this area, see: U.K. House of Commons, Library, *Parliamentary Approval for Military Action*, Briefing Paper, May 8, 2018.

Canadian legislative context: CSIS and CSE

244. Prior to 1984, the RCMP Security Service was responsible for investigating and countering threats to Canada's national security. Over time, the RCMP's Security Service was increasingly subject to criticism on the grounds that it abused its powers and lacked accountability. Between 1966 and 1981, six major commissions of inquiry examined the RCMP Security Service's activities. The most important of these was the McDonald Commission (1981), which recommended a new institutional architecture to ensure greater accountability over the RCMP Security Service. Among the chief areas of concern for the McDonald Commission was the lack of a legislative mandate for the organization. The Commissioner stated:

> We think that a point in Canadian history has been reached when both the requirements of security and the requirements of democracy would be best served by embodying the mandate of Canada's security intelligence agency in an Act of Parliament. . . . A service of this importance must not be left to be regulated, as it is now, by administrative guidelines. Parliamentary democracy requires that a government service of this importance be explicitly approved by the Parliament of Canada.[112]

245. In response to the McDonald Commission, the Canadian government enacted the *Canadian Security Intelligence Service Act*. The Act provided for the creation of CSIS with a statutory mandate to collect, analyze, and retain intelligence "respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada."[113] Among other things, the Act defines key terms, such as "threats to the security of Canada"; describes CSIS's duties and functions; imposes specific limitations on its activities; provides an authority mechanism, judicial warrants, to fulfill its duties and defines the information that must be provided to satisfy the Court; and provides for independent review of CSIS activities.[114] Over the years, CSIS has received ministerial direction to ensure the governance and accountability of the organization, and has elaborated legal requirements for its activities through policies and procedures.

246. Providing a statutory footing for national security and intelligence activities that had previously been conducted under the Crown prerogative has not been done solely in response to abuses of power or authority by a security agency. The evolution of CSE's authority structure from the Crown prerogative to a statutory basis is one such example. The first exercise of the Crown prerogative that created CSE occurred in 1946, when the government issued a secret order in council that created the Communications Branch of the National Research Council of Canada (the CBNRC). In 1975, a second order in council renamed the CBNRC as the Communications Security Establishment and moved the organization to the National Defence portfolio.[115]

---

[112] Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police ["McDonald Commission"], *Second Report: Freedom and Security Under the Law*, Vol. 1, Part V, Ottawa: Privy Council Office, 1981, p. 893.
[113] *CSIS Act*, R.S.C, 1985, c. C-23, s. 12(1)
[114] *CSIS Act*, section 2, sections 12–20, sections 21–24, and Part III.
[115] CSE, *Before the Beginning; the Examination Unit and the Joint Discrimination Unit*, www.cse-cst.gc.ca/en/about-apropos/history-histoire/before-avant;CSE, *The Beginning: The Communications Branch of the National Research Council*, www cse-cst.gc.ca/en/about-apropos/history-histoire/beginning-histoire; and CSE, *Frequently Asked Questions*. www.cse-cst.gc.ca/en/about-apropos/faq.

247. In 1990, a Special Committee of the House of Commons expressed concern about the substantial powers exercised by CSE in light of the fact it had been established by order in council, and lacked any statutory mandate or limitations. Accordingly, the Special Committee recommended in its report, *In Flux But Not in Crisis*, that CSE be established in statute.[116] In 2001 the Government gave CSE a statutory mandate when it added Part V.1 to the *National Defence Act*, which addressed the Special Committee's earlier recommendations and responded to the need for enhancements to CSE's Crown prerogative-based authorities after the attacks of September 11, 2001.[117] Among other things, Part V.1 of the *National Defence Act* defines key terms, such as foreign intelligence; describes CSE's three-part mandate; imposes specific limitations on its activities; provides an authority mechanism, ministerial authorizations, to permit the interception of private communications while conducting certain activities under its mandate, and imposes conditions that must be satisfied for an authorization to be issued; and provides for independent review of CSE activities.[118] Like CSIS, CSE has received ministerial direction to ensure governance and accountability to its minister, and has fleshed out that direction through policies and procedures to ensure the legal compliance of its activities.

248. When gaps are identified in CSIS or CSE authorities, the responsible ministers bring a proposal to Cabinet for consideration and the Government tables legislative amendments for parliamentary scrutiny. These processes are rigorous. They ensure that ministers may consider the implications for broad government priorities and the specific interests of their departments, and ensure that Parliament may consider broad public policy implications for Canadians. As examples, legislative amendments made in 2015 clarified CSIS authority to perform its duties and functions outside of Canada, and provided CSIS with authority to take measures to reduce threats to the security of Canada.[119] In its present form, Bill C-59 proposes significant changes to the mandate of CSE, including providing CSE with authority to conduct foreign intelligence, and defensive and active cyber operations.

---

[116] House of Commons, Special Committee on the Review of the *Canadian Security Intelligence Service Act and Security Offences Act*, *In Flux But Not in Crisis – Report of the Special Committee on the Review of the CSIS Act and Security Offences Act*, September 1990, Recommendation 87, p. 153.

[117] The then Minister of National Defence testified before the House of Commons Standing Committee on Justice and Human Rights that after September 11, 2001, CSE must change and that, "proposed amendments to the *National Defence Act* . . . will remove significant barriers and enhance CSE's capabilities in foreign intelligence and protection of government systems [and] safeguards applied to CSE's operations to protect the privacy of Canadians would be strengthened even further under this new legislation." House of Commons Standing Committee on Justice and Human Rights, Tuesday, October 23, 2001. Meeting 31, www.ourcommons.ca/DocumentViewer/en/37-1/JUST/meeting-31/evidence.

[118] *National Defence* Act, Part V.I, Communications Security Establishment.

[119] *CSIS Act*, subsection 12.1(1). The Act was amended in 2015 as part of the *Anti-terrorism Act, 2015*, which amended the *CSIS Act* to permit CSIS to take, within or outside Canada, measures to reduce threats to the security of Canada, including measures that are authorized by the Federal Court. It authorizes the Federal Court to make an assistance order to give effect to a warrant issued under that Act. It also creates new reporting requirements for the Service and requires the Security Intelligence Review Committee to review CSIS's performance in taking measures to reduce threats to the security of Canada. Department of Justice, Justice Laws website. *Anti-terrorism Act, 2015*, http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2015_20/page-1.html.

Risks raised by DND/CAF

249. Through several appearances before the Committee and written feedback, DND/CAF raised a number of concerns with creating an explicit statutory framework for defence intelligence:

- **Comparisons to CSIS and CSE are inappropriate.** DND/CAF stated that Committee comparisons between DND/CAF defence intelligence activities and the conduct of intelligence activities by dedicated intelligence organizations, CSIS and CSE, is a "fundamental flaw" of this review, as "DND/CAF does not run an intelligence agency." Comparisons are also inappropriate because, "Intelligence is the primary reason these organizations exist, whereas defence intelligence is but one aspect of the spectrum of activities conducted by DND/CAF in support of military operations and the defence of Canada."[120]
- **The risks inherent in DND/CAF defence intelligence activities are different than those of CSIS and CSE intelligence activities.** DND/CAF stated that "the legislative frameworks of [CSIS and CSE] were created to govern the collection and use of intelligence activities as a result of concerns over the rights of Canadians. These concerns do not exist in the case of DND/CAF given its lack of investigative powers."[121]
- **Risks to the Crown prerogative outside of defence intelligence activities.** DND/CAF stated that displacing the Crown prerogative as the authority basis for defence intelligence risks displacing the prerogative in other areas of defence.[122]
- **Risks to cooperation and information sharing.** DND/CAF stated that a statutory framework for defence intelligence may undermine operational cooperation and information sharing with Canada's closest allies.[123]
- **Risks to operational flexibility.** DND/CAF stated that a statutory framework for defence intelligence may undermine operational flexibility.[124]

NSICOP Assessment

250. The Committee examined the experience of CSIS and CSE as their authority frameworks evolved from Crown prerogative to statute. It also deliberated at length about the risks raised by DND/CAF, concerns that deserve careful consideration. On balance, however, the Committee's review has shown that there are legitimate reasons for considering providing DND/CAF with an explicit statutory basis for the conduct of defence intelligence activities. DND/CAF has one of the largest intelligence programs in Canada, measured by personnel and expenditures. Under that program, DND/CAF conducts "full spectrum" intelligence activities, including intelligence assessment and intelligence collection using

[120] DND, Written submission, Speaking points, and DM/CDS oral comments to NSICOP, November 19, 2018.
[121] DND, "DND/CAF comments on Chapter 4 of Draft NSICOP Report," October 2, 2018.
[122] DND, Deputy Minister, Speaking points, NSICOP appearance, October 2, 2018.
[123] DND, Deputy Minister, Speaking points, NSICOP appearance, October 2, 2018.
[124] DND, Deputy Minister, Speaking points, NSICOP appearance, October 2, 2018. Specifically, the Deputy Minister noted, "Even the most carefully crafted legislation can lead to unintended or unanticipated consequences, and a set of legal authorities that looks sufficient and clear today may not work under the changed – and often unforeseen – operational realities of tomorrow. And if those operational realities create a requirement to amend legislated authorities, the process of making those amendments is lengthy, complex, and rigid. Gaps in legislated authorities could last for years, depriving us of the means to do the job that Canadians expect us to do."

sensitive methods, notably SIGINT, HUMINT, counter-intelligence investigations, and *** – **the only entity in Canada to conduct all activities within a single organization**. Considerable risks are associated with each of those activities, including, in some cases, risks to the rights of Canadians.

251. DND/CAF relies on the Crown prerogative for implicit authority to conduct its defence intelligence activities. Unlike CSIS and CSE, its mandate, authorities, limitations, and accountability mechanisms are unknown to Canadians and have not been subject to parliamentary scrutiny. They are, instead, defined through internal administrative policies. The absence of a statutory basis means that authorities to conduct new defence intelligence activities are similarly not subject to parliamentary scrutiny. Parliament may have exclusive authority over defence, but it has not examined the important issues of authorities for defence intelligence activities or limitations on or expansion of powers. Unlike CSIS and CSE, DND/CAF conducts intelligence activities that are not subject to regular review by an independent and external body. Review can, among other things, strengthen accountability for an organization's compliance with the law. NSICOP believes this absence of a statutory basis is an anomaly in Canada's legislative framework for intelligence.

252. Based on the review of the structures, authorities, and governance of DND/CAF defence intelligence activities, NSICOP believes that providing a statutory basis for defence intelligence activities would entail significant benefits. These benefits include strengthening parliamentary scrutiny over an essentially unknown area of public policy that is critical to Canada's security and sovereignty; clarifying the extent and limitations of DND/CAF authorities; defining key terms; formalizing requirements for interdepartmental consultations; and identifying accountability mechanisms, such as reporting requirements to the Minister and regular and independent review. NSICOP fully recognizes that legislation for defence intelligence activities would have to be carefully crafted to account for DND/CAF's unique mandate, and that its obligations under international law must be taken into consideration.

Conclusion

253. The Committee's focus in this chapter was threefold. The first, to define the nature, scale, and scope of defence intelligence activities; the second, to determine the authority framework under which these activities are conducted; and the third, to determine the governance structure employed by DND/CAF to ensure oversight and accountability of defence intelligence. The Committee made no findings in the first of those areas: it recognizes the vital role that defence intelligence plays in the defence mandate. This is especially true with regard to the planning and conduct of operations, protection of CAF members, and the deployment of forces on operations.

254. The Committee believes that DND/CAF's administrative system of governance over defence intelligence activities is an important component of mitigating risk in intelligence operations and ensuring appropriate control and accountability. That said, the Committee found a number of weaknesses in that system, and has made findings and recommendations that it believes will improve the governance and accountability of DND/CAF defence intelligence activities.

255. With respect to the question of legislation, the Committee has endeavored to present both the risks and the benefits of placing defence intelligence on a statutory footing. The Committee's call for the Government to give serious consideration to legislation is a reflection of its analysis of these important issues.

Findings

256. The Committee makes the following findings:

F8. The development and use of defence intelligence activities involve inherent risks, and require robust measures of control and accountability. The Department of National Defence/Canadian Armed Forces (DND/CAF) has implemented an internal administrative system of governance for the defence intelligence program that includes specific internal oversight bodies, ministerial direction, special authorizations by the Minister of National Defence for the employment of specific intelligence capabilities, and functional direction across its intelligence program.

F9. The governance of the defence intelligence program is lacking in the following areas:

- DND/CAF does not have a standardized process or principles to determine a nexus between an authorized mission and an intelligence activity (paragraph 200);
- the principal internal governance body for defence intelligence, the Defence Intelligence Management Committee, did not fulfill its mandate to enable the Chief of Defence Intelligence to bring forward issues related to sensitive defence intelligence capabilities and relationships to the Deputy Minister and Chief of the Defence Staff (paragraph 216);
- DND/CAF has made limited effort to measure and document compliance with the obligations of the Ministerial Directive on Defence Intelligence. The new Directorate of Intelligence Review, Compliance and Disclosure and the Defence Intelligence Oversight Board will be important in this respect (paragraph 217);
- the annual reports to the Minister of National Defence on defence intelligence activities do not report on challenges or gaps in the oversight of defence intelligence, and are silent on compliance with respect to key aspects of the Ministerial Directive on Defence Intelligence that deal with identified areas of risk (paragraphs 215–217); and
- DND/CAF does not have a standardized process for interdepartmental consultations (paragraph 233).

F10. The defence intelligence program has been subject to internal audits and evaluations, which have resulted in recommendations that have been implemented by DND/CAF. There is, however, no dedicated, external and ongoing review of DND/CAF defence intelligence activities. Neither NSICOP, nor the proposed NSIRA, is required to conduct regular reviews of DND/CAF defence intelligence activities.

F11. In Canada's legislative framework for national security and intelligence, DND/CAF is an anomaly in conducting its intelligence activities under the Crown prerogative. Those activities are similar in kind, risk, and sensitivity to those conducted by other Canadian security and intelligence organizations, which operate under and benefit from clear statutory authorities, limitations and requirements for ongoing review, tailored to the requirements of their specific mandates.

Recommendations

257. The Committee makes the following recommendations:

R5. The Department of National Defence/Canadian Armed Forces (DND/CAF) review and strengthen its administrative framework governing defence intelligence activities, particularly with respect to the Ministerial Directive on Defence Intelligence, to ensure that it meets its own obligations on governance and reporting to the Minister of National Defence, and is properly tracking the implementation of those obligations. In particular:

- devise a standard process, or principles, for determining a nexus between a defence intelligence activity and a legally authorized mission;
- document its compliance with obligations in the Directive, including in areas of risk specified in the Directive not currently included in annual reports to the Minister; and
- implement a standardized process for interdepartmental consultations on the deployment of defence intelligence capabilities, including minimum standards of documentation.

R6. The Government amend Bill C-59, *An Act respecting national security matters*, to ensure that the mandate of the proposed National Security and Intelligence Review Agency includes an explicit requirement for an annual report of DND/CAF activities related to national security or intelligence.

R7. Drawing from the Committee's assessment and findings, the Government give serious consideration to providing explicit legislative authority for the conduct of defence intelligence activities.

Addendum: 2019 Special Report on DND/CAF collection of information on Canadians as part of the defence intelligence program

258. On October 26, 2018, DND/CAF provided the Committee with a new Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information, which was promulgated on August 31, 2018. DND/CAF did not provide this new directive proactively, despite its clear relevance to the terms of reference for the NSICOP review DND/CAF defence intelligence activities. DND/CAF stated that not providing the functional directive was an oversight, an explanation that the Committee accepts.

259. Nonetheless, NSICOP believes that the subject of this functional directive is of considerable importance and merits further analysis as part of DND/CAF's broader suite of directives and policies concerning defence intelligence activities. NSICOP also believes that additional study of the DND/CAF defence intelligence program will be of benefit to an ongoing evaluation of the authority structure and governance of the defence intelligence program. The Committee has therefore decided to finalize this chapter of its Annual Report and conduct a separate review of DND/CAF authority and directives to collect, use, retain, and disseminate information and intelligence on Canadians as part of defence intelligence activities.

260. Pursuant to Section 21(2) of the *NSICOP Act*, the Committee will provide a Special Report to the Prime Minister and the Minister of National Defence in 2019.

Appendix A: Ministerial Directive on Defence Intelligence

TO: Deputy Minister of National Defence
Chief of the Defence Staff

MINISTERIAL DIRECTIVE ON DEFENCE INTELLIGENCE

I. Preamble

1. Defence intelligence is an essential and integral part of Canadian Forces (CF) operations, whether conducted at home or abroad, in peacetime and during armed conflict. Defence intelligence is also an essential enabler for the Department of National Defence (DND)'s core responsibilities, such as research and development, capability development and defence procurement. Finally, defence intelligence is a critical component of the Government of Canada (GoC)'s ability to make informed decisions in matters concerning national defence, national security and foreign affairs.

2. Recent years have seen a proliferation of new state and non-state threats against Canada, and a closer interconnection between the roles and responsibilities of DND/CF and those of other GoC departments and agencies, as well as those of our partners and allies around the world. This strategic shift, combined with rapid growth in the global use of – and dependence on – new technologies has made the context of modern military operations far more complex.

3. As a result of these changes, not only has the very nature of the support provided by defence intelligence changed, but the successful administration of that support has become more important than ever. Therefore, to help ensure the continued effectiveness and accountability of defence intelligence programs and activities, this document provides high-level direction and guidance with respect to the ongoing development of a clear and comprehensive governance framework.

4. The following directive is issued under Ministerial authority pursuant to section 4 of the *National Defence Act* (NDA) and provides direction to the Deputy Minister (DM) and to the Chief of the Defence Staff (CDS) concerning their separate but complementary responsibilities and accountabilities in relation to defence intelligence. This directive does not apply to criminal intelligence, which exists as a separate and distinct discipline under the purview of the CF Provost Marshal and the Military Police.

5. Further Ministerial Directives will be issued as necessary to provide additional guidance on defence intelligence matters. Both the DM and CDS are encouraged to advise the Minister of circumstances where additional directives would benefit defence intelligence.

II. Policy Statement

6. In accordance with the Minister's direction on the establishment of intelligence priorities, the DND/CF may develop, generate and employ such intelligence capabilities as are required to enable lawful, timely and effective decisions and actions in support of:

a. the core roles and missions of the CF, including the planning and execution of routine and contingency operations carried out in the defence of Canada, the defence of North America in cooperation with the United States, and the promotion of international peace and security;

b. CF capability development and force generation activities, and all supporting DND responsibilities, such as research and development and defence procurement; and,

c. lawful requests for defence intelligence support from external stakeholders.[*]

III. Authority, Mandate and Mission

7. The legal authority to conduct defence intelligence activity, as is the case for all defence activities, is firmly established in Canadian legislation (i.e. the *National Defence Act*), international law and elements of the common law (including the Crown Prerogative). However, any means and methods used in the conduct of defence intelligence activities remain subject to applicable Canadian and international laws, as well as GoC and Ministerial policies and directives.

8. The authority to conduct defence intelligence activities requires that:

a. there be a clear nexus between the nature and scope of the defence intelligence activity and DND/CF's mandated defence operations or activities; or,

b. in cases where defence intelligence support is provided in response to a lawful request from an external stakeholder, that the support comply with the same mandate and authorities that govern the receiving body.

IV. Accountability and Responsibility of the CDS for Defence Intelligence

9. The CDS is accountable to the Minister for the control and administration of the CF, including both the means used and results achieved in the planning and execution of CF operations and intelligence activities. The CDS is also accountable for the development and force generation of CF capabilities – including defence

[*] For the purposes of this directive, "external stakeholders" shall include, but not necessarily be limited to, federal and provincial authorities and Canada's international partners and allies.

intelligence capabilities – in support of the present and future effectiveness of the CF. This entails the responsibility for the CDS to exercise strict oversight and control of defence intelligence activities conducted by the CF, in accordance with the obligations and limitations contained in all applicable Canadian and international laws, GoC and Ministerial policies and directives.

V. Accountability and Responsibility of the DM for Defence Intelligence

10. The DM is accountable to the Minister for the provision of sound policy advice in respect of all defence intelligence matters, both in support of the Minister's individual accountabilities to Parliament, as well as his or her broader responsibilities to the GoC. This includes advice on the alignment of defence intelligence activities with wider GoC policies and initiatives and on matters of international defence relations.

11. Under the *Financial Administration Act*, the DM is responsible for the prudent management of departmental programs and resources – including those allocated to defence intelligence. As the accounting officer for DND/CF, the DM is required by law to provide information and explanations to appropriate Parliamentary committees on how resources have been organized and allocated to deliver the defence intelligence program, and in so doing to assist Parliament in holding the government to account.

VI. Role of the Commander Canadian Forces Intelligence Command / Chief of Defence Intelligence

12. Under the direction of the CDS and the DM, the Commander Canadian Forces Intelligence Command (Comd CFINTCOM) / Chief of Defence Intelligence (CDI) serves as the functional authority for all defence intelligence activity across DND/CF.

13. In addition to being directly and solely accountable to the CDS for the effective leadership and administration of the Canadian Forces Intelligence Command (CFINTCOM) and all of its subordinate units, the Comd CFINTCOM / CDI provides oversight and direction on all defence intelligence activities across DND/CF, including deployed operations, consistent with departmental and CF priorities.

14. The Comd CFINTCOM / CDI is jointly accountable to the DM and the CDS for:

a. providing functional guidance and direction governing the development, generation and employment of defence intelligence capabilities;

b. monitoring the implementation of that functional direction;

c. managing defence intelligence arrangements with external stakeholders; and,

d. producing both scheduled and *ad hoc* reports on compliance with functional direction, identifying any issues of concern or potential concern, and making recommendations relating to any corrective action that may need to be taken.

15. In fulfilling the role of the functional authority for defence intelligence, the Comd CFINTC◉M / CDI helps ensure DND/CF adherence to, and compliance with all applicable Canadian and international laws, GoC and Ministerial policies and directives, as well as orders and directives issued by the CDS to the CF.

VII. Direction to the DM and the CDS

16. It is imperative that the governance and accountability of defence intelligence activity keep pace with the ongoing evolution of intelligence activity and of GoC security and intelligence community standards. The DM and the CDS must work together to ensure that appropriate policies, directives and oversight structures are developed and implemented to maintain the maximum possible responsiveness, effectiveness and accountability of defence intelligence. This governance and accountability framework must include provisions for support to any review mechanism for defence intelligence that may be developed. The Minister will provide further guidance on the development of any such mechanism as appropriate.

17. In accordance with their respective responsibilities and accountabilities, and to ensure the continued accountability of defence intelligence, the DM and the CDS must exercise rigorous oversight and sound judgement in considering or authorizing the development or use of defence intelligence capabilities. They must also ensure that the Minister remains properly informed of defence intelligence activities in accordance with his or her mandate as described in the *National Defence Act*, as well as his or her broader responsibilities as a Minister of the Crown.

18. The CDS and/or the DM must undertake appropriate interdepartmental and legal consultations before authorizing or initiating any defence intelligence activity that they consider to be particularly sensitive, or that is likely to present a significant impact on any of the following areas:

a. national security and the sovereignty of Canada;

b. any serious threat to the lives and/or legal or Constitutional rights of persons in Canada and Canadian citizens around the world, or to the rights of individuals more broadly as recognized by international law;

c. any serious threat to the protection and/or advancement of Canada's foreign relations and reputation abroad;

d. any potential risk of exposure, real or perceived, of the GoC, DND or CF to any significant domestic or international legal liability, or to

circumstances that would contravene the DND/CF Code of Values and Ethics; and,

e. all matters or activities which may entail significant financial commitments outside of GoC-approved investments and expenditures.

19. Furthermore, the DM and CDS must ensure that DND/CF carry out appropriate interdepartmental consultations, including with the Department of Foreign Affairs, Trade and Development, before entering into any defence intelligence-related arrangements with foreign governments, organizations or multilateral bodies. They must ensure that the Minister is properly informed of any new international defence intelligence arrangements that are made, as well as any substantial modifications to the nature or scope of any existing arrangements.

20. In accordance with their respective responsibilities and accountabilities, the DM and/or CDS may refer the decision on whether to authorize a specific defence intelligence activity or arrangement to the Minister as they consider it appropriate, taking into account the responsibilities and mandate of the Minister as described in the *National Defence Act* and as a Minister of the Crown.

21. Finally, the DM and CDS must provide an annual report to the Minister on defence intelligence governance, performance, strategic priorities, major program and special project initiatives, and any policy, legal and management issues of significance. The Minister will rely on the information and advice provided in these reports in fulfilling his or her accountabilities to Parliament, responsibilities to the Prime Minister and to Cabinet, and in communicating with the public and media regarding matters of defence intelligence.

22. This directive shall remain in effect until further notice.

Le ministre de la Défense nationale

Hon. Rob Nicholson, PC, QC, MP
Minister of National Defence

Chapter 5: Observations on NSICOP's Inaugural Year and Looking Forward

261. NSICOP's inaugural year was marked by learning and adjustment for the Committee, its Secretariat and the security and intelligence community.

262. Members of the security and intelligence community provided support to the Committee throughout its first year. The Communications Security Establishment and the Canadian Security Intelligence Service used their long experience working with review bodies to help other organizations prepare for Committee reviews. Community officials were generous with their time and readily shared their experience with the Committee. Their support for NSICOP's mandate was repeatedly expressed during site visits, briefings and Committee hearings. A number of organizations also identified specific personnel or established dedicated units to respond to heightened expectations of review (the Department of National Defence was notable in this regard), which will be important should Bill C-59 receive Royal Assent and the National Security and Intelligence Review Agency be established in the future. For its part, the Privy Council Office supported the Committee and its Secretariat to put in place the administrative, physical and information infrastructure required to conduct their work. It has taken a coordination and liaison role on behalf of the community, leading the coordination of the community's briefings to the Committee and responding to its requests for information.

263. The Committee's timelines imposed pressures on the security and intelligence community. The Committee did not start meeting until December 2017, and did not have a fully staffed Secretariat until August 2018. Before it could determine which reviews it would conduct in its first year, the Committee had to learn about the many organizations involved in the complex fields of security and intelligence. As discussed in Chapter 1, it conducted a number of site visits to the core organizations of the security and intelligence community and was briefed on the national security threats and challenges facing Canada. In April 2018, it deliberated on the range of reviews it could conduct and chose two, described in this report. It also agreed to conduct a special review of the various allegations surrounding the Prime Minister's trip to India in February 2018. In each case, the Committee imposed tight timelines on the departments and agencies to provide information and hold hearings to ensure the Committee could provide the Prime Minister with its Special Report and Annual Report, consistent with the requirements of the *NSICOP Act*.

264. The Committee recognizes that these were not ideal circumstances. In the future, the Committee intends to take a more measured approach to its reviews. Without compromising its independence or the ambition of its work, the Committee will endeavor to engage community members earlier to better define the scope of reviews and determine the information that will be required; to set reasonable deadlines for the provision of documents, working level engagement and to prepare for Committee hearings; and to work earlier with officials to determine the scope of changes required of Committee reports to protect information that should not be publicly disclosed. These steps will not always be possible in every circumstance – as the Committee learned early in its mandate, a special report may come up unexpectedly and require an accelerated timetable or unique information requirements. But where the steps are possible, the Committee believes they will help to strengthen its reviews.

265. At the same time, the Committee notes a number of challenges which it will monitor over time. One challenge relates to the provision of information. Despite unambiguous and, the Committee believes, sincere expressions of support from the leaders of the security and intelligence community for the mandate of NSICOP, several organizations interpreted Committee requests for information narrowly. The Committee had to return repeatedly to organizations to obtain more information, including relevant email correspondence, to ensure that what was provided was complete, and to engage officials for answers to basic questions.

266. The Committee would be remiss not to comment on its own challenges. Most sadly, the Committee lost one of its own, Member of Parliament Gordon Brown, to an untimely death in May 2018. Gord's passing deprived us of a wise and considered voice on issues of importance to Parliamentarians and Canadians. The implications of his absence grew more significant over the summer and fall as the Committee deliberated on its two major reviews. They grew acute with the resignation of the Honourable Tony Clement on November 7, depriving the Committee of any representation from the Official Opposition in the House of Commons. While the majority of the Committee's work was finished by early November, these episodes underlined the importance of quickly identifying replacements for NSICOP Members, whenever they leave and for whatever reason. It also caused the Committee to reconfirm its own discipline on appropriately handling sensitive and classified information and adhering to personal security measures, including receiving additional briefings in November from security and intelligence officials in these areas.

Future work

267. In addition to the planned Special Report noted in the previous chapter, the Committee has already initiated its review work for its 2019 Annual Report. The Committee believes it is important to address a key gap in Canada's security and intelligence community by examining organizations not previously subject to review (i.e., outside of CSE, CSIS and the RCMP). Its 2018 review of the defence intelligence activities of DND/CAF was a first step. In 2019, the Committee will review the national security and intelligence activities of the CBSA. The Committee's review of CBSA will focus on understanding what role it plays in Canada's security and intelligence community, delineating its national security and intelligence activities from its broader responsibilities, and understanding how those activities work in practice. This review will continue to build a picture of the various parts of the security and intelligence community and how it works together, and to identify future areas for review.

268. The Committee also decided to review the issue of foreign interference. Canada's experience and that of our closest allies over the past several years shows that some states are taking increasingly aggressive measures to influence our political processes and institutions, behaviour which poses a threat to our democratic values and security. As a pluralistic state composed of immigrant communities, Canada is not immune from these threats and must be particularly vigilant against efforts by foreign states to threaten or manipulate those communities for their own purposes. In 2019, the Committee will study the threat posed by foreign interference to Canada's security and the measures in place to counter it.

269. Inspired by the recent work of the UK Intelligence and Security Committee, the Committee has decided to look more closely at issues of diversity and inclusion in the security and intelligence community. These issues are important: Canada's population should see itself reflected in its public service. They are even more vital for security and intelligence organizations, which must ensure that their analysis and advice is informed by the broadest range of perspectives and experiences and to ensure that their investigations are conducted by people who understand the communities and people involved. Starting in 2019, the Committee will track how the security and intelligence community is doing in this area and engage officials from that community to identify best practices and areas where more could be done.

Conclusion

270. The Committee has an important mandate and responsibilities. Through the course of its work over the last year, the Committee sought to build its understanding of the security and intelligence community and to create productive relationships with the officials who lead it. The Committee is convinced that its reviews will, over time, strengthen the functioning and accountability of Canada's security and intelligence community and contribute to Canadians' knowledge of this important area of government.

Annex A: List of Findings

Chapter 3

F1. The process for setting intelligence priorities has a solid foundation and overall participation by the community has made it more rigorous, inclusive, and systematically applied.

F2. Coordinating the timing and consistency of Ministerial Directions to organizations involved in the intelligence priorities process would add rigour to the process, strengthen the development of the Standing Intelligence Requirements, and increase the accountability of ministers.

F3. The great number of Standing Intelligence Requirements, particularly at the highest priority level, makes it difficult for the community to ensure that Cabinet has the information it needs on the significance of identified gaps in collection and assessment.

F4. In general, the internal processes that NSICOP examined were effective and enforced.

F5. The delay by CSIS in updating its internal Intelligence Requirements Document to incorporate the new intelligence priorities and SIRs in a timely manner undermined the accountability of both the Minister of Public Safety and Emergency Preparedness and Cabinet, and weakened the accountability of the overall system to support those priorities.

F6. The National Intelligence Expenditure Review methodology is not applied consistently by organizations to provide Cabinet with complete and comparable information on how organizational resources are used across government to respond to the intelligence priorities.

F7. Performance measurement for the security and intelligence community is not robust enough to give Cabinet the context it needs to understand the efficiency and effectiveness of the security and intelligence community.

Chapter 4

F8. The development and use of defence intelligence activities involve inherent risks, and require robust measures of control and accountability. The Department of National Defence/Canadian Armed Forces (DND/CAF) has implemented an internal administrative system of governance for the defence intelligence program that includes specific internal oversight bodies, ministerial direction, special authorizations by the Minister of National Defence for the employment of specific intelligence capabilities, and functional direction across its intelligence program.

F9. The governance of the defence intelligence program is lacking in the following areas:

- DND/CAF does not have a standardized process or principles to determine a nexus between an authorized mission and an intelligence activity (paragraph 200);
- the principal internal governance body for defence intelligence, the Defence Intelligence Management Committee, did not fulfill its mandate to enable the Chief of Defence Intelligence to bring forward issues related to sensitive defence intelligence capabilities and relationships to the Deputy Minister and Chief of the Defence Staff (paragraph 216);

- DND/CAF has made limited effort to measure and document compliance with the obligations of the Ministerial Directive on Defence Intelligence. The new Directorate of Intelligence Review, Compliance and Disclosure and the Defence Intelligence Oversight Board will be important in this respect (paragraph 217);
- the annual reports to the Minister of National Defence on defence intelligence activities do not report on challenges or gaps in the oversight of defence intelligence, and are silent on compliance with respect to key aspects of the Ministerial Directive on Defence Intelligence that deal with identified areas of risk (paragraphs 215–217); and
- DND/CAF does not have a standardized process for interdepartmental consultations (paragraph 233).

F10. The defence intelligence program has been subject to internal audits and evaluations, which have resulted in recommendations that have been implemented by DND/CAF. There is, however, no dedicated, external and ongoing review of DND/CAF defence intelligence activities. Neither NSICOP, nor the proposed NSIRA, is required to conduct regular reviews of DND/CAF defence intelligence activities.

F11. In Canada's legislative framework for national security and intelligence, DND/CAF is an anomaly in conducting its intelligence activities under the Crown prerogative. Those activities are similar in kind, risk, and sensitivity to those conducted by other Canadian security and intelligence organizations, which operate under and benefit from clear statutory authorities, limitations and requirements for ongoing review, tailored to the requirements of their specific mandates.

Annex B: List of Recommendations

Chapter 3

R1. The National Security and Intelligence Advisor, supported by the Privy Council Office, invest in and take a stronger managerial and leadership role in the process for setting intelligence priorities to ensure organizational responses to the intelligence priorities are timely and consistently implemented.

R2. The security and intelligence community develop a strategic overview of the Standing Intelligence Requirements to ensure Cabinet is receiving the best information it needs to make decisions.

R3. Under the leadership of the National Security and Intelligence Advisor and supported by the Privy Council Office, the security and intelligence community develop tools to address the coordination and prioritization challenges it faces in relation to the Standing Intelligence Requirements.

R4. The security and intelligence community, in consultation with the Treasury Board Secretariat, develop a consistent performance measurement framework that examines how effectively and efficiently the community is responding to the intelligence priorities, including a robust and consistent resource expenditure review.

Chapter 4

R5. The Department of National Defence/Canadian Armed Forces (DND/CAF) review and strengthen its administrative framework governing defence intelligence activities, particularly with respect to the Ministerial Directive on Defence Intelligence, to ensure that it meets its own obligations on governance and reporting to the Minister of National Defence, and is properly tracking the implementation of those obligations. In particular:

- devise a standard process, or principles, for determining a nexus between a defence intelligence activity and a legally authorized mission;
- document its compliance with obligations in the Directive, including in areas of risk specified in the Directive not currently included in annual reports to the Minister; and
- implement a standardized process for interdepartmental consultations on the deployment of defence intelligence capabilities, including minimum standards of documentation.

R6. The Government amend Bill C-59, *An Act respecting national security matters*, to ensure that the mandate of the proposed National Security and Intelligence Review Agency includes an explicit requirement for an annual report of DND/CAF activities related to national security or intelligence.

R7. Drawing from the Committee's assessment and findings, the Government give serious consideration to providing explicit legislative authority for the conduct of defence intelligence activities.

Annex C: Committee Outreach and Engagement

Site Visits:

Canada Border Services Agency
Canadian Security Intelligence Service
Communications Security Establishment
Department of National Defence/Canadian Armed Forces
Global Affairs Canada
Integrated Terrorism Assessment Centre
Royal Canadian Mounted Police

Committee Meetings and Hearings:

Canadian Security Intelligence Service

- Director
- Assistant Director, Intelligence
- Deputy Director General, Intelligence Assessment Branch

Communications Security Establishment

- Chief
- Head, Canadian Centre for Cyber Security
- Deputy Chief of IT Security
- Director General, Policy, Disclosure and Review
- Director General, Intelligence Operations
- Director, Client Engagement
- Director, Policy and Review

Department of Finance

- Associate Assistant Deputy Minister
- Director of Financial Crimes Governance and Operations

Department of Justice

- Deputy Assistant Deputy Minister

Department of National Defence/Canadian Armed Forces

- Deputy Minister of National Defence
- Chief of the Defence Staff
- Vice Chief of the Defence Staff
- The Judge Advocate General
- Assistant Chief of Defence Intelligence
- Strategic Joint Staff, Director General Operations
- Assistant Deputy Minister, Policy
- Senior General Counsel and Legal Advisor to the DND/CAF

- Commander, Canadian Joint Operations Command
- Commander, Canadian Forces Intelligence Command and Chief of Defence Intelligence
- Executive Director, National Security and Intelligence Review and Oversight of Compliance Secretariat

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)

- Director and Chief Executive Officer
- Assistant Director of Collaboration, Development and Research

Global Affairs Canada

- Deputy Minister
- Director General, Counter-Terrorism, Crime and Intelligence
- Chief of Protocol
- Director General, South Asia Relations Bureau
- Assistant Deputy Minister, International Security and Political Affairs
- Director General, Middle East Bureau
- Executive Director, Threat Assessment and Intelligence Service

Immigration, Refugees and Citizenship Canada

- Associate Assistant Deputy Minister, Strategic and Program Policy
- Director General, International Network

Integrated Terrorism Assessment Centre

- Executive Director
- Director General, Policy and Programs

Office of the Privacy Commissioner of Canada

- Privacy Commissioner of Canada
- Director of Policy, Research and Parliamentary Affairs
- Acting Director of the Government Advisory Directorate
- Chief of Staff to the Privacy Commissioner

Privy Council Office

- National Security and Intelligence Advisor to the Prime Minister
- Foreign and Defence Policy Advisor to the Prime Minister
- Assistant Secretary to the Cabinet, Security and Intelligence
- Director of Operations, Security and Intelligence
- Director, Strategic Policy and Planning, Security and Intelligence
- Senior Policy Analyst, Strategic Policy and Planning, Security and Intelligence
- Chief Security Officer and Executive Director, Security and Operations
- Executive Director, Intelligence Assessment Secretariat
- Acting Director, Middle East/Africa Division, Intelligence Assessment Secretariat

Public Safety Canada

- Deputy Minister
- Senior Assistant Deputy Minister, National and Cyber Security Branch
- Director General, National Security Operations Directorate

Royal Canadian Mounted Police

- Commissioner
- Deputy Commissioner, Federal Policing

Security Intelligence Review Committee

- SIRC Committee members
- Executive Director

Treasury Board Secretariat

- Associate Secretary
- Assistant Secretary, International Affairs, Security and Justice
- Executive Director , International Affairs, Security and Justice; Defence and Immigration Division
- Executive Director, International Affairs, Security and Justice; Security and Justice Division

Allies:

United Kingdom

- 7 Members of the Intelligence and Security Committee of Parliament
- Director, ISC Secretariat
- Analysts, ISC Secretariat
- Political Officer, British High Commission in Ottawa

Australia

- Members of the Parliamentary Joint Committee on Intelligence and Security

Civil Rights Organizations:

- Amnesty International Canada
- British Columbia Civil Liberty Associations
- Ligue des droits et libertés du Québec

Academics

- Wesley Wark
- Craig Forcese

Private Sector

- Ron Nehring

Annex D: Glossary

ADM	Assistant Deputy Minister
CBSA	Canada Border Services Agency
CDI	Chief of Defence Intelligence
CDS	Chief of the Defence Staff
CRCC	Civilian Review and Complaints Commission of the RCMP
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DIMC	Defence Intelligence Management Committee
DND/CAF	Department of National Defence / Canadian Armed Forces
Five Eyes	Allied nations of Canada, the United States, the United Kingdom, Australia and New Zealand
IRCC	Immigration, Refugees and Citizenship Canada
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIA	National Security and Intelligence Advisor to the Prime Minister
NSIRA	National Security and Intelligence Review Agency
OCSEC	Office of the Communications Security Establishment Commissioner
PCO	Privy Council Office
RCMP	Royal Canadian Mounted Police
SIRC	Security Intelligence Review Committee
SIRs	Standing Intelligence Requirements
TBS	Treasury Board Secretariat