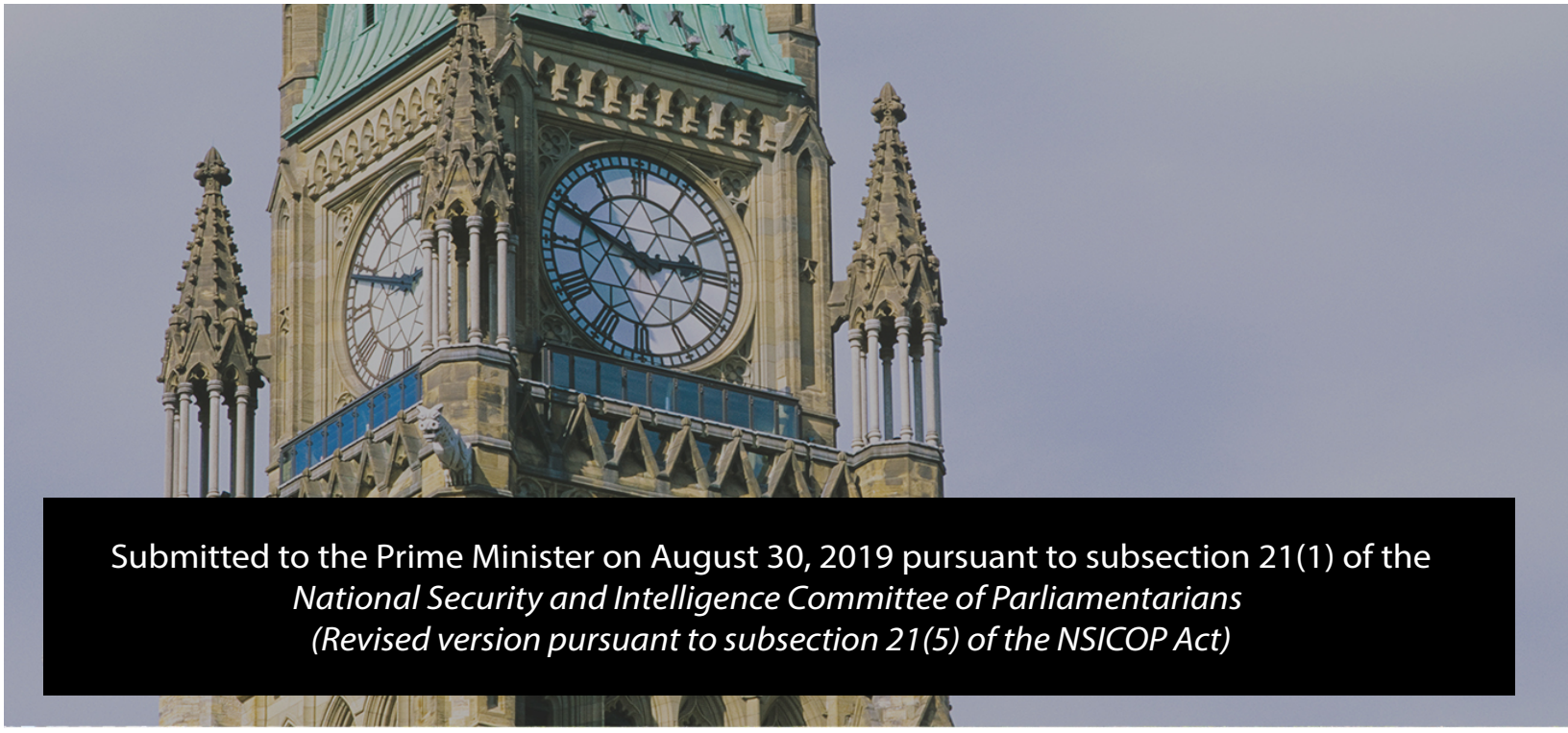
National Security and Intelligence Committee of Parliamentarians

Annual Report 2019



Submitted to the Prime Minister on August 30, 2019 pursuant to subsection 21(1) of the *National Security and Intelligence Committee of Parliamentarians*
(Revised version pursuant to subsection 21(5) of the NSICOP Act)

Canada

Ottawa, ON.

The National Security and Intelligence Committee of Parliamentarians

Annual Report 2019 (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP100E (Print)
ISSN 2562-5101 (Print)

CP100E-PDF (Online)
ISSN 2562-511X (Online)

Cette publication est également disponible en français :
Rapport annuel 2019 (Version révisée selon le paragraphe 21(5) de la *Loi sur le CPSNR*)

ANNUAL REPORT 2019

The National Security and Intelligence Committee of Parliamentarians

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

Submitted to the Prime Minister on August 30, 2019
Revised version tabled in Parliament in March 2020

Revisions

Consistent with subsection 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 NSICOP Act, the Prime Minister may, after consulting the Chair of the Committee, direct the Committee to submit to him or her a revised version of the 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 Annual Report provided to the Prime Minister on 30 August 2019. Revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national defence and national security, 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. ***]

Chair's Message

Ottawa, ON – August 30, 2019

The past year was an important milestone for the National Security and Intelligence Committee of Parliamentarians (NSICOP, or 'the Committee'). In March, the Committee welcomed two new members from the Official Opposition in the House of Commons. In April, the Prime Minister tabled the Committee's first Annual Report in Parliament. The Committee conducted significant outreach activities thereafter, including with the media and academics. As the Chair of the Committee, I participated in the Open Government Partnership Global Summit in May 2019 to discuss oversight and review in the Canadian national security landscape. Also in May, I appeared before the House of Commons Standing Committee on Public Safety and National Security, and in June I joined two Senators from the Committee to appear before the Senate Standing Committee on National Security and Defence. Several members of the Committee and the Executive Director of the Secretariat provided presentations on the Committee's mandate and work at a number of Canadian universities. The Committee believes this outreach helps to build Canadians' understanding of national security and intelligence.

The year was marked by an ambitious agenda and significant changes. Based on its experience in drafting its first Annual Report, the Committee adjusted its approach to conducting reviews and engaged more closely with members of the security and intelligence community to develop the Committee's agenda and to identify the most relevant documents. Starting in late 2018 and continuing into January 2019, the Committee launched four new reviews, three of which are described in this Annual Report and the fourth in a Special Report to the Prime Minister and the Minister of National Defence. For the Committee, these reviews required significant investments of time and effort to understand topics of significant complexity and diversity. For the organizations of the security and intelligence community, they required significant work to provide documents and prepare officials for appearances. The Committee recognizes the work of all organizations in this year's review process and thanks them for their efforts.

Reflections on the past years

This Report will be the Committee's last before it is dissolved with the drop of the writ for the 2019 federal election. While much of what the Committee learned and experienced is reflected in its reports, there are a number of issues worth highlighting at the end of its term. The first is that the Committee has been gratified by the extensive feedback provided by academics and stakeholders from across Canada. This engagement reinforces for the Committee the value of reviewing issues of importance to Canadians' security, rights and freedoms, and of speaking frankly to Canadians about how the

government is addressing those issues. We hope that our work this year continues to inform public debate.

Government response to the Committee's findings and recommendations

The Committee provided two reports to the Prime Minister in 2018. The first was a Special Report on allegations related to national security arising from the Prime Minister's trip to India in February 2018. That report was provided to the Prime Minister and the Ministers of Foreign Affairs and Public Safety and Emergency Preparedness on October 12, 2018. The second was the Committee's Annual Report, which included its findings and recommendations from two reviews it conducted over the course of 2018: a review of how the government establishes its intelligence priorities, and a review of the defence intelligence activities of the Department of National Defence and the Canadian Armed Forces. The Annual Report was provided to the Prime Minister on December 21, 2018. The two reports contained a total of 29 findings (18 and 11, respectively) and 12 recommendations (5 and 7, respectively). The government has responded to these reports by stating that they have resulted in reflection and analysis across the Government of Canada, and the recommendations continue to be actively reviewed and considered.

Significant challenges encountered by the security and intelligence community

Over the past two years, the Committee had numerous opportunities to hear from security and intelligence officials about the challenges they face in executing their respective and collective mandates. While the Committee did not conduct reviews of these issues, four are worthy of mention here:

- Countries around the world continue to adapt their cyber operations to serve their national interests and to protect their own information assets. Over the past several years, Canada has made significant changes to its own cyber posture in response to evolving threats and new technologies.
- The ability of intelligence organizations to provide intelligence to other government organizations for subsequent use (for example, to pursue a criminal investigation) continues to be impeded by significant legal, policy, operational and organizational challenges (intelligence to evidence).
- The capacity of federal police and security organizations to address increasingly complex, global and sophisticated crime has diminished with the diversion of resources to other priorities, notably terrorism, the attrition of experienced police investigators, and rapid changes in information and other technologies.
- The ability of police and intelligence organizations to obtain information under existing legal authorities has steadily diminished with the evolution of information technology, eroding those organizations' ability to investigate and disrupt or prosecute criminal and security threats.

These issues may merit review in the future.

A work in progress

The Committee has had the opportunity to reflect on the lessons, challenges and highlights of the past two years. Canada is one of the last G7 countries to have set up a Parliamentary review body, with access to classified information to examine national security and intelligence activities from a strategic perspective. The foundations of broad, independent review of national security and intelligence in Canada are still being established and will be further expanded with the recent creation of the National Security and Intelligence Review Agency. In that context, the Committee expected that some 'growing pains' would accompany its establishment. In its first Annual Report shortly after its creation in 1984, the Security Intelligence Review Committee (SIRC) acknowledged that while "its function may create an adversarial relationship [with CSIS] in certain circumstances, it is also very conscious of the need to establish a solid foundation of trust between the two organizations."[1]

NSICOP's efforts to establish this trust with the security and intelligence community has required constant monitoring, dialogue and regular stock-taking. From the first meetings with the Committee, senior government officials have indicated their support for the mandate and work of NSICOP and have been readily available to meet on specific reviews and more general wide-ranging discussions.

The legislation that gives NSICOP its mandate, its right of access to information needed to conduct its reviews, and the limitations to that right of access, is clear. Sub-section 13(1) of the NSICOP Act states, "...the Committee is entitled to have access to any information that is under the control of a department and that is related to the fulfilment of the Committee's mandate." However, the NSICOP Act does not give the Committee authority to impose deadlines or force the provision of information, relying instead on the good faith of the organizations under review, and a clear and common understanding of the Committee's mandate. In most cases, departments provided the requested information in a comprehensive and timely manner. However, the Committee has faced a number of challenges in accessing information based on reasons that are inconsistent with NSICOP's enabling legislation. Some organizations provided summaries of information requested rather than the original records, inconsistently applied the restriction of information subject to Cabinet Confidences, or failed to provide records that the Committee considered relevant to its reviews.

As has been observed on many occasions, the Committee is conscious that its work plan and schedule have placed significant demands and pressure on the individual organizations. In the future, adjustments on both sides will be necessary.

The challenges outlined above have been communicated to the National Security and Intelligence Advisor (NSIA) to the Prime Minister. As the coordinator for the security and intelligence community, the NSIA is in a position to ensure that the community has the capacity and consistent approach to meet

---

[1] The Security Intelligence Review Committee Annual Report 1984-85.

its responsibilities and obligations towards the Committee. For its part, NSICOP is committed to taking stock of lessons learned and to formalizing the procedures for Committee meetings and reviews. The Committee remains hopeful that the conduct of its reviews will continue to improve and takes due notice of the issues above in contemplation of the mandatory five-year review of the NSICOP Act in 2022.

Acknowledgements

Committee members would like to express their sincere thanks and appreciation to the staff of the Secretariat. Their role is, to quote the NSICOP Act, to "assist the Committee in fulfilling its mandate." Without their dedication and professional support, the Committee would not have been able to meet over 70 times, nor produce two Annual Reports and two Special reports, within a two-year period.

In closing I would also like to acknowledge and thank my Parliamentary colleagues on the Committee. On behalf of all Canadians, members shared a common commitment to improving the performance and accountability of the security and intelligence community, and in doing so, demonstrated the value of a non-partisan approach to issues of profound importance to Canadians: their security, personal rights and freedoms.

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)

The Hon. Percy Downe, Senator

Mr. Emmanuel Dubourg, M.P.

The Hon. Diane Finley, P.C., M.P.

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

Ms. Gudie Hutchings, M.P.

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

The Hon. Rob Nicholson, P.C., Q.C., M.P.

Mr. Murray Rankin, M.P.
(resigned August 1, 2019)

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

March 9, 2020

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 our Annual Report for 2019. The Report includes the three substantive reviews completed by the Committee in its second year of activity, namely diversity and inclusion in Canada's security and intelligence community; the government response to foreign interference; and, the national security and intelligence activities of the Canada Border Services Agency. The unanimous Report includes nineteen findings and eight recommendations to improve the accountability and effectiveness of national security and intelligence in Canada.

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

Yours sincerely,

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

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

TABLE OF CONTENTS

Introduction

1. The National Security and Intelligence Committee of Parliamentarians (NSICOP or "the Committee") is pleased to present the Prime Minister with its 2019 Annual Report. The Committee has a broad mandate to review the framework and activities of Canada's security and intelligence community. Members of the Committee hold the highest security clearances and, with certain exceptions, have the legislative right to access any information related to their mandate that is under the control of a department.

2. Consistent with sub-section 8(1) of the NSICOP Act, the Committee's mandate is to review:

- the legislative, regulatory, policy, administrative and financial framework for national security and intelligence ('framework reviews');
- any activity carried out by a department that relates to national security or intelligence ('activity reviews');
- any matter relating to national security or intelligence that a minister of the Crown refers to the Committee ('referral reviews').

In both 2018 and 2019, the Committee conducted at least one framework review and one activity review. This approach allowed the Committee to analyze national security and intelligence issues that implicated the security and intelligence community as a whole, while also conducting reviews of agencies and departments previously not subject to external review. Consistent with subsection 21(2) of the NSICOP Act, the Committee may also provide the Prime Minister and the Minister concerned with a special report on any matter related to its mandate. The Committee conducted two reviews during this period, which arose from unique circumstances that, in the Committee's opinion, required Special Reports to the responsible Ministers.

3. In 2019, the Committee maintained an ambitious agenda, building on the foundation established in its first year. As part of this 2019 Annual Report, the Committee conducted two framework reviews (Diversity and Inclusion in the Security and Intelligence Community, and the Government Response to Foreign Interference) and one activity review (the Canada Border Services Agency's National Security and Intelligence Activities). The Committee also produced a Special Report on the collection, use, retention and dissemination of information on Canadians in the context of the Department of National Defence and Canadian Armed Forces (DND/CAF) defence intelligence activities.

4. Between January and June, the Committee met 22 times, including to hear testimony from 44 officials from 8 organizations, 1 former senior official and 3 academics. The Committee finalized its four reviews over a further three meetings in July and August.

5. Pursuant to paragraph 21(1)(d) of the NSICOP Act, the Committee must include in its Annual Report the number of instances in the preceding year that an appropriate minister determined that an activity review would be injurious to national security. As outlined in paragraphs 16(1)(a) and 21(1) of

the Act, the Committee is also required to disclose the number of times a responsible minister refused to provide information to the Committee due to his or her opinion that the information constituted special operational information or would be injurious to national security. In 2019, no reviews proposed by the Committee were deemed injurious to national security and no information requested by the Committee was refused by a minister on those grounds.

6. The Committee also notes that it received annual reports from Canada Border Services Agency, Canadian Security Intelligence Service, Communications Security Establishment and Royal Canadian Mounted Police on their application of Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities.

Format of the annual report

7. Chapter 1 presents the Committee's review of diversity and inclusion in the Canadian security and intelligence community. Challenges to increasing diversity and inclusion — two core values of Canada and its public service — persist in the security and intelligence community despite decades of legislation, multiple reports and repeated calls for change. These issues are of particular importance for organizations responsible for protecting national security and the rights and freedoms of Canadians. This review provides a baseline assessment of the degree of representation of women, Aboriginal peoples, members of visible minorities and persons with disabilities within the security and intelligence community, and examines the goals, initiatives, programs and measures departments and agencies have taken to promote diversity and inclusion. It is the first multi-departmental review of its kind.

8. Chapter 2 presents the Committee's review of the government's response to foreign interference. This review demonstrates that some states pose a risk to Canadian institutions and Canadian rights, freedoms and values. The chapter's first section explains the breadth and scope of the threat of foreign interference. It outlines the primary threat actors and examines the threat that those actors pose to Canada's fundamental institutions and ethno-cultural communities. The second describes government efforts to respond to the threat. This review is important because of the potential adverse effects of foreign interference on Canadian democratic institutions and on the rights and freedoms of Canadians.

9. Chapter 3 presents the Committee's review of the national security and intelligence activities of the Canada Border Services Agency (CBSA), a core member of Canada's security and intelligence community, given its responsibility for border security. However, CBSA's national security and intelligence activities are not widely known nor well understood. These activities also present a number of inherent risks, including risks to an individual's Charter rights and risks related to balancing enforcement and the free-flow of legitimate travellers and trade. Based on these considerations and others, the Committee conducted the first-ever review of CBSA's most sensitive national security and intelligence activities.

Chapter 1: Diversity and Inclusion in the Security and Intelligence Community

Introduction

Rationale and overview

10. Canada is a multicultural country with a diverse population and evolving demographics. Currently, immigrants make up two-thirds of population growth, the Aboriginal population is growing four times as fast as the non-Aboriginal population,[1] 22 percent of people aged 15 years and over have a disability, and up to 13 percent of people self-identify as LGBT.[2] The government estimates that by 2031, members of visible minorities will represent almost one third of Canadians.[3] Canada's public service must adapt to these changes. As the Clerk of the Privy Council stated, "Ours is a Public Service that draws strength from diversity and inclusion. Ours is a Canada whose every voice deserves to be heard."[4]

11. Diversity and inclusion are two core values of the public service. According to the Joint Union/Management Task Force on Diversity and Inclusion of the Treasury Board of Canada Secretariat (TBS), "a **diverse** workforce in the public service is made up of individuals who have an array of identities, abilities, backgrounds, cultures, skills, perspectives and experiences that are representative of Canada's current and evolving population. An **inclusive** workforce is fair, equitable, supportive, welcoming and respectful. It recognizes, values and leverages differences in identities, abilities, cultures, skills, experiences and perspectives that support and reinforce Canada's evolving human rights framework."[5][Emphasis added.]

12. In addition to their normative value, diversity and inclusion have tangible benefits for organizational performance. A 2018 study of over 1,700 companies in eight countries by the Boston

---

[1] This review uses the term 'Aboriginal Peoples,' consistent with the *Constitution Act, 1982* and the *Employment Equity Act*, and which includes the Indian, Inuit and Métis peoples in Canada. However, the Committee recognizes and respects that 'Indigenous Peoples' has become the preferred terminology. See: https://laws-lois.justice.gc.ca/eng/acts/e-5.401/page-2.html#docCont.

[2] Lesbian, Gay, Bisexual, Transgender. This statistic does not include people who identify as Queer or Two Spirit. See: Statistics Canada, "Population growth: Migratory increase overtakes natural increase," *The Daily*, May 17,2018; Statistics Canada, "Aboriginal peoples in Canada: Key results from the 2016 Census," *The Daily*, October 25, 2017; Statistics Canada, "A demographic, employment and income profile of Canadians with disabilities aged 15 years and over, 2017," Canadian Survey on Disability Reports, November 28, 2018; and Treasury Board Secretariat (TBS), *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017, www.canada.ca/en/treasury-board-secretariat/corporate/reports/building-diverse-inclusive-public-service-final-report-joint-union-management-task-force-diversity-inclusion.html.

[3] TBS, *Progress Update: Joint Union/Management Task Force on Diversity and Inclusion in the Public Service*, 2017, www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/task-force-diversity-inclusion/progress-update-task-force-diversity-inclusion.html.

[4] Ian Shugart Clerk of the Privy Council and Secretary to Cabinet, "Message to Public Servants from the new Clerk of the Privy Council," April 23, 2019, www.canada.ca/en/privy-council/news/2019/04/a-message-to-public-servants-from-the-new-clerk-of-the-privy-council.html.

[5] TBS, *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017, www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/task-force-diversity-inclusion/progress-update-task-force-diversity-inclusion.html.

Consulting Group and the Technical University of Berlin, found that there was a "statistically significant relationship between diversity and innovation outcomes in all countries examined," suggesting that "diversity represents a tangible missed opportunity and significant potential upside."[6] Multiple academic and professional studies have reached similar conclusions.[7] A large part of this missed opportunity is talent. TBS notes that there are systemic and attitudinal barriers to women, members of visible minorities, persons with disabilities and Aboriginal peoples in the Public Service.[8] Removing these barriers will result in a more representative and diverse workforce and will ensure that organizations are leveraging the broad range of perspectives and talent that Canada has to offer.

13. Reports on allied security and intelligence communities similarly recognize the value of a diverse workforce and an inclusive work environment. A 2017 report commissioned by the U.S. Director of National Intelligence stated, "there is no more important place to encourage and support a culture of diversity and inclusion than in today's Intelligence Community." The report noted that increasing diversity "expands the talent base and more accurately reflects analytic capabilities necessary to evaluate and meet mission requirements."[9] A report on gender diversity commissioned by the Australian Federal Police in 2016 pointed to the increasingly complex threats facing security organizations as requiring a diverse workforce with "a breadth of skills, expertise and talent."[10] The U.K. Intelligence and Security Committee of Parliament made similar findings in 2018, stating, "if all intelligence professionals are cut from the same cloth, then they are likely to share 'unacknowledged biases' that circumscribe both the definition of the problems and the search for solutions."[11] Finally, a 2015 Central Intelligence Agency study on diversity in leadership noted that increasing diversity,

---

[6] Rocio Lorenzo and Martin Reeves, "How and Where Diversity Drives Financial Performance," *Harvard Business Review*, January 30, 2018.

[7] See for example: Vivian Hunt, et. al, "Delivering through Diversity," *McKinsey & Company*, January 2018; Bessma Momani and Jillian Stirk, "Diversity Dividend: Canada's Global Advantage," *Canadian Centre for International Governance*, 24 April 2017; Vivian Hunt, et. al., "Diversity Matters," *McKinsey & Company*, February 2015; Report from the Panel on Labour Market Opportunities for Persons with Disabilities, *Rethinking Disability in the Private Sector: We all have abilities. Some are just more apparent than others*, 2013; Credit Suisse, "Gender diversity and corporate performance," *Credit Suisse Research Institute*, 2012; Katherine W. Philips, "How Diversity Makes Us Smarter," *Scientific American*, October 1, 2014; and European Commission, *The Costs and Benefits of Diversity*, October 2003.

[8] Section 2 of the *Employment Equity Act* designates four employment equity groups: women, Aboriginal peoples, persons with disabilities and members of visible minorities. For the purposes of this review, the terms used to refer to designated groups are the same as they appear in the Act. NSICOP Secretariat consultation with TBS, Acting Manager Employment Equity, Diversity and Inclusion, Office of the Chief Human Resources Officer, February 5, 2019; and TBS, *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017, www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/task-force-diversity-inclusion/progress-update-task-force-diversity-inclusion.html.

[9] United States, Intelligence Community Equal Employment Opportunity and Diversity Office, "Diversity and Inclusion: Examining Workforce Concerns within the Intelligence Community," January 2017, https://fas.org/irp/dni/diversity.pdf.

[10] Elizabeth Broderick, "Cultural Change: Gender Diversity and Inclusion in the Australian Federal Police," Elizabeth Broderick and Co., 2016.

[11] UK, Intelligence and Security Committee, *Diversity and Inclusion in the UK Intelligence Community*, September 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/740654/20180718_Report_Diversity_and_Inclusion.pdf.

particularly at senior levels, helps to promote "the Agency as an employer of choice in an increasingly diverse nation."[12]

14. Canada's national security and intelligence community also acknowledges the critical importance of a diverse and inclusive workforce to operational success. A 2010 report commissioned by the Canadian Security Intelligence Service (CSIS) highlighted that greater diversity and inclusion at CSIS would enhance the organization's ability to attract talent and establish relationships with diverse communities in Canada.[13] The report also noted that a diverse and inclusive workplace would allow CSIS to leverage "cultural competencies, language skills, generational characteristics, gender, community connections . . . to continuously improve how the Service gathers intelligence, counters terrorism and protects Canada's national security."[14]

15. The Committee decided to review diversity and inclusion in the security and intelligence community for several reasons. Most importantly, challenges to increasing diversity and inclusion persist in the security and intelligence community even after decades of legislation, multiple reports and repeated calls for change. This is most evident in the Canadian Armed Forces and the Royal Canadian Mounted Police, which have settled class action lawsuits alleging widespread harassment, violence and discrimination, and at CSIS, which settled a lawsuit specifically alleging Islamophobia, racism and homophobia. The Committee agrees with the analysis of security and intelligence organizations abroad and in Canada on the importance of diversity and inclusion. These issues are particularly important for organizations responsible for protecting the national security of Canada and the rights and freedoms of Canadians. A review across organizations in this field has never been conducted. This review falls under the Committee's mandate to examine the legislative, regulatory, policy, administrative and financial framework for national security and intelligence.

16. The Committee focused on the Canada Border Services Agency (CBSA); CSIS; the Communications Security Establishment (CSE); the Department of National Defence (DND) and the Canadian Armed Forces (CAF);[15] Global Affairs Canada (GAC); the Integrated Terrorism Assessment Centre (ITAC); the Privy Council Office (PCO); Public Safety Canada; and the Royal Canadian Mounted Police (RCMP).[16] These organizations work as a close community. In its review, therefore, the Committee sought to understand the individual circumstances of each organization, but also to identify challenges they face as a community and where they have made collective efforts to address common problems.

---

[12] Central Intelligence Agency, "Director's Diversity in Leadership Study: Overcoming Barriers to Advancement," April 17, 2015, www.cia.gov/library/reports/dls-report.pdf.

[13] Judy Laws and Denise McLean, "Public Safety and Emergency Preparedness Canada (PSEPC) Diversity Roadmap Project," *Graybridge Malkam*, June 15, 2010.

[14] Judy Laws and Denise McLean, "Public Safety and Emergency Preparedness Canada (PSEPC) Diversity Roadmap Project," *Graybridge Malkam*, June 15, 2010.

[15] The Department of National Defence (DND) and the Canadian Armed Forces (CAF) includes the civilian (DND) and uniformed (CAF) portions of the workforce. DND and CAF are treated as two distinct organizations in this report because they are separate legal entities and have differing legislated reporting requirements.

[16] In its 2018 Annual Report, NSICOP listed these organizations – with the exception of Public Safety Canada – as "core members of the security and intelligence community." NSICOP, *Annual Report* 2018, April 2019.

Objectives of the review

17. This review provides a baseline assessment of the degree of representation of women, Aboriginal peoples, members of visible minorities and persons with disabilities within the security and intelligence community, and examines the goals, initiatives, programs and measures that departments and agencies have taken to promote diversity and inclusion.

18. Many of the diversity and inclusion goals of the organizations under review are part of a long-term government-wide strategy for representation and cultural change. This review is intended to establish a baseline of diversity and inclusion in the security and intelligence community from which the Committee may conduct a more comprehensive assessment in three to five years. The first section examines the legislative and policy framework for diversity and inclusion, and the current representation of women, Aboriginal peoples, members of visible minorities and persons with disabilities across each organization under review. The second section assesses the different ways in which organizations across the community promote diversity and foster inclusion in their workforce.

Methodology

19. For this review, the Committee requested information from the organizations under review dating primarily, but not exclusively, from the period of January 1, 2015, to March 31, 2018. The Committee received the first documents in early February 2019. The Committee conducted an initial analysis of the information provided and requested further information in April. This review is based on over 5,000 pages of documentation, departmental consultations and independent research. The Committee notes the following limitations to its review:

- The Committee did not hold hearings in the context of this review, but the NSICOP Secretariat consulted with departments, agencies, academics and stakeholders from January to May 2019 on the Committee's behalf.
- The Committee did not conduct focus groups with employees or examine individual cases of current or former staff of the security and intelligence community. Instead, it conducted an analysis of the data and other information provided by departments and agencies.
- Due to an absence of more granular data, some of the information assessed in this review applies to departments or agencies as a whole, rather than employees or units that work in specific areas of security and intelligence.

Diversity and employment equity

20. According to the TBS Joint Union/Management Task Force, diversity is the array of identities, abilities and backgrounds of individuals who make up a workforce.[17] The principle of employment equity, in turn, ensures that individuals identified within the four employment equity groups (women, Aboriginal peoples, persons with disabilities and members of visible minorities) are given fair and equal access to employment opportunities.[18] This section provides an overview of employment equity requirements and the current state of diversity in the security and intelligence community. It presents the main legislative and policy direction for all departments in the federal public service, as well as their planning and monitoring requirements. It also describes the current representation of designated groups in each organization under review and challenges related to the accuracy of those figures.

Legislative, policy and accountability framework

21. The legislative framework for diversity and inclusion in the security and intelligence community comprises several acts and regulations.[19] For the purposes of this review, the most important is the *Employment Equity Act*.[20] This Act designates four employment equity groups: women, Aboriginal peoples, persons with disabilities and members of visible minorities.[21] It requires employers to identify and eliminate barriers to employment for these groups, institute positive policies and practices, and make reasonable accommodations to achieve a degree of representation in each occupational category and group.[22] Beyond legislation, a number of government-wide policies and documents may also contribute to the achievement and maintenance of diversity and inclusion. Three are of particular importance: ministerial mandate letters, priorities and initiatives of the Clerk of the Privy Council, and "gender-based analysis plus" (GBA+).

---

[17] TBS, *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017, www.canada.ca/en/treasury-board-secretariat/corporate/reports/building-diverse-inclusive-public-service-final-report-joint-union-management-task-force-diversity-inclusion.html.

[18] *Employment Equity Act*, S.C. 1995, c. 44, s. 2.

[19] The primary legislation governing diversity and inclusion are the *Canadian Charter of Rights and Freedoms*, the *Canadian Human Rights Act*, the *Employment Equity Act*, and the *Public Service Employment Act*. Other legislation, such as the *Official Languages Act*, the *Financial Administration Act*, and the *Canada Labour Code*, also play a role.

[20] CAF is governed under specific Employment Equity Regulations with certain exemptions related to operational requirements. See: *Employment Equity Act*, 1995 and *Canadian Forces Employment Equity Regulations*, SOR/2002-421.

[21] For the purposes of this review, the Committee uses the terms for each designated group as they appear in the *Employment Equity Act*.

[22] Occupational category refers to the broad job category, such as "scientific and professional" or "administrative and foreign service." Occupational group refers to the specific job such as "engineering" or "program administration." See: Canada, *Guide to allocating positions using the occupational group definitions* for further information on job functions of specific occupational groups, www.canada.ca/en/treasury-board-secretariat/services/collective-agreements/occupational-groups/guide-allocating-positions-using-occupational-group-definitions.html.

Ministerial mandate letters

22. Mandate letters are one of the main mechanisms for the Prime Minister to establish key expectations and priorities. For the period under review, the Prime Minister directed all ministers responsible for organizations in the security and intelligence community to "help ensure gender parity and that Indigenous Canadians and minority groups are better reflected in positions of leadership."[23] Of particular importance to the security and intelligence community, the Prime Minister directed the Minister for Women and Gender Equality to "work with the President of the Treasury Board and the Clerk of the Privy Council to increase the number of women in senior decision-making positions across government, particularly in central agencies and in our **security services**."[24] [Emphasis added.]

Priorities and initiatives of the Clerk of the Privy Council

23. As the head of the public service, the Clerk of the Privy Council identified diversity and inclusion as a priority. In 2018, the Clerk established the Clerk's Table on Diversity and Inclusion to serve as a forum for advice on improving diversity and inclusion across the public service.[25] The Clerk also convenes the Task Force on Diversity and Inclusion and the Deputy Minister Task Team on Harassment.[26]

Gender-based analysis plus (GBA+)

24. In 1995, the government committed to using an analytical process called gender-based analysis (GBA) to advance gender equality in Canada. In 2014–2015, the government expanded this analytical process beyond gender considerations to incorporate intersecting identity factors.[27] This new process is called GBA+. According to Women and Gender Equality Canada, GBA+ "is an analytical process used to assess how diverse groups of women, men and non-binary people may experience policies, programs and initiatives. The 'plus' in GBA+ acknowledges that GBA goes beyond biological (sex) and socio-cultural (gender) differences. We all have multiple identity factors that intersect to make us who we are; GBA+ also considers many other identity factors, like race, ethnicity, religion, age, and mental or physical disability."[28] GBA+ is used to evaluate specific plans and initiatives and, increasingly, internal organizational practices.

---

[23] Excerpt included in mandate letters for: Minister of Public Safety and Emergency Preparedness (November 12, 2015), Minister of Foreign Affairs (February 1, 2017) and Minister of National Defence (November 12, 2015).
[24] Mandate letter for the Minister of Status of Women (October 4, 2017).
[25] See: Canada, "Clerk's Table on Diversity and Inclusion," www.canada.ca/en/privy-council/corporate/clerk/table-diversity-inclusion.html.
[26] See: Canada, "Deputy Minister Committees," www.canada.ca/en/privy-council/corporate/clerk/table-diversity-inclusion.html; and Canada, "Safe Workspaces: Starting a dialogue and taking action on harassment in the Public Service," 2018, www.canada.ca/content/dam/pco-bcp/documents/clk/Harrassment-Report_EN.pdf.
[27] Laura Munn-Rivard, "Gender-based Analysis Plus in Canada," *HillNotes*, Library of Parliament, May 26, 2017, https://hillnotes.ca/2017/05/26/gender-based-analysis-plus-in-canada/.
[28] Status of Women Canada, "What is GBA+?," https://cfc-swc.gc.ca/gba-acs/index-en.html.

Planning, monitoring and reviewing

25. Under the various legislative, regulatory and policy frameworks, departments and agencies are required to plan, monitor and review their progress on employment equity.

Planning

26. According to the *Employment Equity Act*, departments and agencies within Canada's federal public service must prepare employment equity plans.[29] An employment equity plan is a strategic document where departments and agencies identify trends in the representation of designated groups and outline their approach to achieving specific employment equity goals. The plans are to include policies to correct underrepresentation, measures being taken to remove barriers to employment and short-term (one to three years) and long-term (more than three years) numerical goals for the hiring and promotion of designated group members.[30] All of the organizations under review provided their most recent employment equity plans, which highlighted the importance of a representative workforce and their commitment to fostering an inclusive work environment.[31]

27. These plans differ in timing and approach. A majority of organizations under review – namely CBSA, CSIS, CSE, GAC and Public Safety Canada – produce employment equity plans every three-years. DND and the RCMP's last employment equity plans expired in 2017. The CAF's most recent employment equity plan covers a period of five years, from 2015 to 2020. In their approach to numerical goal setting, the CAF and the RCMP established ambitious long-term objectives to increase the overall representation of designated groups. CSIS and GAC, in turn, set short-term targets for representation in specific occupational groups, while others – including CBSA, DND and Public Safety Canada – set the more conservative target of closing representation gaps.

Monitoring

28. Departments and agencies are required to monitor the implementation of their plan and periodically review their progress. According to the *Employment Equity Act*, organizations must provide information on the representation of designated group members overall and within occupational groups, their salary ranges, and information regarding the hiring, promotion and terminations of designated group members to the President of the Treasury Board each fiscal year.[32] TBS compiles this information and tables an annual report on the status of employment equity in the public service in

---

[29] *Employment Equity Act*, S.C. 1995, c. 44, s. 10(1).
[30] *Employment Equity Act*, S.C. 1995, c. 44, ss. 10(2)-(3).
[31] As an example, in its 2015–2020 employment equity plan, the CAF notes that "While the *Employment Equity Act (EEA)* imposes a legislative requirement to address under-representation for persons in the designated groups, the broader issues of creating and fostering a more diverse CAF is an organizational priority, both today and for the future." DND/CAF, *Canadian Armed Forces Employment Equity Plan 2015–2020*, undated.
[32] *Employment Equity Act*, S.C. 1995, c. 44, s. 21(1),(2), (3) and (4).

Parliament.[33] Organizations have different reporting requirements and have adopted different approaches to monitoring, which complicates efforts to assess and compare progress between employment equity plans.

29. As separate agencies, the CAF, CSIS, CSE and the RCMP are required to submit annual employment equity reports to TBS.[34] The reports were inconsistent in terms of the type of information included and the degree of analysis conducted. For example, employment equity reports provided by CSE included detailed information and analysis of salary ranges for each designated group, while the employment equity report from CSIS included only the general distribution of designated groups across levels in the organization.[35] Similarly, a majority of reports focused their workforce analysis on general trends in representation of equity groups with little contextual analysis.[36] In contrast, the RCMP's *2017–2018 Employment Equity Report* included a comprehensive analysis of the representation of designated groups and highlighted concentrations of designated group members in specific occupational categories.[37]

30. TBS no longer requires organizations in the core public service, including CBSA, DND, GAC, PCO and Public Safety Canada, to produce annual reports.[38] These organizations have adopted different approaches to monitoring progress in achieving their employment equity goals. GAC, for example, substituted these reports with detailed monitoring documents tracking the implementation of its employment equity plan.[39] Public Safety Canada produced regular updates on the status of the implementation of its plan.[40] CBSA, DND and PCO did not provide the Committee with additional monitoring reports for their employment equity plans.

---

[33] The TBS annual report on the status of employment equity in the public services does not include information from separate agencies, including the CAF, CSIS, the Communications Security Establishment (CSE) and Regular Members of the RCMP. *Employment Equity Act*, S.C. 1995, c. 44, s. 21(1).

[34] TBS, Written communication from the Manager of Employment Equity, Diversity and inclusion, Office of the Chief Human Resources Officer, June 14, 2019.

[35] CSE, *Employment Equity Annual Report 2017–2018,* undated.

[36] For example, the workforce analysis in CAF's 2017–2018 Employment Equity Report notes increases and decreases in representation for each designated group as compared to the previous year. Similarly, the workforce analysis conducted in CSIS's 2017–2018 Employment Equity Report notes trends in overall representation of designated groups in the past five years. See: CAF, *Canadian Armed Forces Employment Equity Report 2017–2018*, undated; and CSIS, *Annual Report to the Treasury Board of Canada – Employment Equity Program 2017/2018*, September 2017.

[37] RCMP, *RCMP Employment Equity Annual Report 2017–2018*, undated.

[38] TBS, Written communication from the Manager of Employment Equity, Diversity and inclusion, Office of the Chief Human Resources Officer, April 25, 2019.

[39] GAC, *Employment Equity Action Plan April 1, 2014 – March 21, 2017: Monitoring Report April 1, 2014 to January 15, 2017*, undated.

[40] Public Safety Canada, The 2016–2019 PS Diversity and Employment Equity Action Plan Accomplishments of 2016–2017, 2017; and Privy Council Office (PCO), *PCO's Employment Equity and Diversity Plan 2014–2015 Progress Report and the 2016–2019 Plan*, April 12, 2016.

Review

31. Under Canada's *Employment Equity Regulations*, when an employer identifies underrepresentation of a designated group, it is required to conduct a review of its employment systems, policies and practices to identify possible employment barriers.[41] While the regulations do not specify a period during which organizations should conduct this review, the absence of regular reviews means organizations may not have sufficient data to identify problems or identify responsive measures. While all of the organizations under review have identified consistent gaps in representation of one or many designated groups, the frequency of their employment systems reviews differed. CSE, GAC, PCO and Public Safety Canada conducted an employment systems review within the last three years. It has been more than five years since the following organizations conducted their most recent employment systems reviews: CAF (2013), CBSA (2010), CSIS (2011) and DND (2010).[42]

LGBTQ2+ individuals in the security and intelligence community

LGBTQ2+ individuals are not covered under the *Employment Equity Act*. The Committee does not, therefore, include this group in this review. However, the Committee notes that TBS included, for the first time, questions on self-identification for LGBTQ2+ on the Public Service Employee Survey 2018 in anticipation of LGBTQ2+ being added as a designated group in the future. Given the legacy of discrimination against LGBTQ2+ members in the security and intelligence community, the potential future designation of this group will be an important issue to be addressed by the organizations under review.[43]

---

[41] *Employment Equity Regulations*, SOR/96-470, 8 and 9, https://laws-lois.justice.gc.ca/eng/regulations/sor-96-470/page-2.html#h-5.

[42] DND and CAF are currently conducting an employment systems review. DND/CAF, Diversity & Inclusion Review – Supplementary information from DND/CAF, April 23, 2019.

[43] In November 2017, the Prime Minister officially apologized for the government's treatment of the LGBTQ2+ community from the 1950s to the 1990s. The legacy of this discrimination was particularly acute in the security and intelligence community, where there was a concerted effort on the part of the Security Service for over two decades to collect information on homosexuals. Prime Minister of Canada, "Remarks by Prime Minister Justin Trudeau to apologize to LGBTQ2 Canadians," 28 November 2017, https://pm.gc.ca/eng/news/2017/11/28/remarks-prime-minister-justin-trudeau-apologize-lgbtq2-canadians. See also, McDonald Commission, *Freedom and Security Under the Law*, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police: Second Report, Volume 2, 1981.

Representation of designated groups in the security and intelligence community, 2017–2018

32. Most organizations in the security and intelligence community identify representation gaps in their own workforce according to workforce availability (WFA) estimates. The most recent WFA estimates are calculated using data from the 2011 Canadian Household Survey and the 2012 Canadian Survey on Disability related specifically to Canadian citizens' fields of study and previous work experience. This data is used to estimate the availability of designated groups for each occupational category across the Canadian workforce. The RCMP uses labour market availability (LMA) estimates to determine representation gaps by looking at a segment of the workforce, including individuals who are not Canadian citizens, defined by geography, level of education and qualifications.[44] The CAF also uses LMA estimates, but does not account for geography and includes only Canadian citizens aged 18 to 49 with at least a grade 10 education.[45] Statistics for LMA are calculated using data from the 2011 Canadian Household Survey and the 2012 Canadian Survey on Disability. WFA and LMA estimates are different for each organization under review, because the skills and experience required for each occupational category and group differ across organizations. Nonetheless, broad comparisons are possible.

33. Table 1 presents the average representation of designated groups across the public service, and shows, in each of the organizations under review, the representation of these groups overall and at the executive level as of 2017–2018. **It is important to note that the numbers represent the designated groups for all staff in the organizations under review. The figures therefore also include individuals who do not work in the field of national security and intelligence.** The information in Table 1 is analyzed by organization on the subsequent pages.

---

[44] RCMP, *RCMP Employment Equity Annual Report 2017–2018,* 2018.

[45] DND/CAF written communication to NSICOP, July 5, 2019.

Departments and Agencies		Women				Aboriginal Peoples				Members of Visible Minorities				Persons with Disabilities			
Public Service Average		Workforce Availability (WFA)		Current		WFA		Current		WFA		Current		WFA		Current	
		52.5%		54.8%		3.4%		5.1%		13%		15.7%		4.4%		5.3%	
Organizations Under Review		WFA	Current	EX WFA	EX Current	WFA	Current	EX WFA	EX Current	WFA	Current	EX WFA	EX Current	WFA	Current	EX WFA	EX Current
Canadian Armed Forces (CAF)		14.5%	15.0%	Not available (n/a)	7.2%	3.4%	2.8%	n/a	0.9%	6.0%	7.2%	n/a	2.0%	n/a	n/a	n/a	n/a
Canada Border Services Agency (CBSA)		44.4%	47.5%	45.5%	37.1%	4.1%	3.3%	5.9%	2.4%	11.9%	14.7%	8.5%	8.4%	4.4%	3.4%	2.3%	2.7%
Canadian Security Intelligence Service (CSIS)		47.3%	48.5%	47.3%	40.0%	2.6%	2.3%	2.6%	2.0%	18.5%	16.5%	18.5%	7.0%	4.6%	4.2%	4.6%	3.0%
Communications Security Establishment (CSE)		36.7%	37.3%	27.6%	30.4%	1.8%	2.0%	2.5%	4.3%	21.5%	11.4%	8.6%	4.3%	4.2%	3.7%	5.9%	0.0%
Department of National Defence (DND)		39.5%	40.0%	43.5%	42.4%	2.6%	3.1%	3.5%	<5	8.7%	7.8%	11.2%	4.1%	4.6%	5.4%	2.4%	5.9%
Global Affairs Canada (GAC)		57.6%	55.3%	51.4%	42.5%	3.1%	4.6%	5.0%	4.0%	13.9%	20.3%	9.5%	11.9%	3.9%	3.6%	2.3%	3.0%
Integrated Terrorism Assessment Centre (ITAC)		47.3%	68.0%	47.3%	67.0%	2.6%	5.0%	2.6%	0.0%	18.5%	13.0%	18.5%	0.0%	4.6%	5.0%	4.6%	0.0%
Privy Council Office (PCO)		52.2%	57.3%	47.1%	52.27%	1.8%	2.9%	n/a	0.0%	12.7%	13.0%	9.2%	4.5%	4.0%	3.4%	2.3%	4.5%
Public Safety Canada		55.3%	61.1%	46.3%	54.9%	3.1%	4.2%	6.6%	8.5%	15.1%	11.0%	7.5%	7.0%	3.9%	5.9%	2.3%	2.8%
Royal Canadian Mounted Police (RCMP)	Total	48.0%	39.5%	n/a	n/a	4.0%	6.8%	n/a	n/a	18.0%	12.0%	n/a	n/a	5.0%	2.4%	n/a	n/a
	Regular Member	49.3%	21.6%	52.1%	21.8%	3.1%	7.8%	2.8%	8.4%	15.1%	11.1%	12.7%	5.8%	n/a	1.7%	n/a	0.7%
	Civilian Member	48.0%	51.7%	52.1%	56.4%	4.0%	3.9%	2.8%	1.7%	18.0%	13.6%	12.7%	7.7%	5.0%	2.7%	2.8%	0.9%
	Public service employee	48.0%	77.6%			4.0%	5.7%			18.0%	13.7%			5.0%	4.1 %		

Table 1: Representation of Designated Groups in Organizations in the Security and Intelligence Community, 2017–2018

Notes for Table 1: Representation of Designated Groups in Organizations in the Security and Intelligence Community (2017–2018)

- The green boxes indicate representation that is above workforce availability (WFA) or labour market availability (LMA) and the red boxes indicate representation that is below WFA or LMA. Grey boxes indicate that information is not available to assess whether representation is above or below WFA or LMA.
- The data for Public Safety Canada is dated March 2017. The data across the public service and for each of the other organizations under review dates from 2017–2018.
- "Current" means the representation of each designated group across all occupational categories and groups. "EX" means "executive" and includes relatively small numbers of individuals, meaning that percentages fluctuate noticeably with the addition of one individual.
- Data for DND and CAF is listed separately for the two organizations because they report separately on employment equity representation for civilian (DND) and military (CAF) members.
- CAF data includes regular force members only (not reserves). TBS established a compensation benchmark for CAF equivalents for the EX cadre: Colonel/Captain (Navy), Brigadier General/Commodore, Major-General/Rear-Admiral and Lieutenant-General/Vice Admiral.[46]
- The CAF is not required to set employment equity goals for persons with disabilities due to operational requirements and the principle of the Universality of Service, which requires that CAF members be "physically fit, employable and deployable for general operational duties."[47]
- The RCMP's workforce is composed of Regular Members (RM), Civilian Members (CM) and public service employees (PSE). Due to operational requirements, the RCMP is not required to set employment equity goals for persons with disabilities for the RM category.[48]

Sources:

- Data on the average representation of designated groups across the public service: TBS, *Employment Equity in the Public Service of Canada 2017–2018*, May 2019, p. 6, www.canada.ca/en/government/publicservice/wellness-inclusion-diversity-public-service/diversity-inclusion-public-service/employment-equity-annual-reports/employment-equity-public-service-canada-2017-2018.html;
- CAF, *Employment Equity Report 2017–2018*, undated, p. 4;
- CBSA, "Employment Equity Data (April 2015-October 2018)," October 2018;
- CSIS, "Designated Groups as of 2018-03-31," January 2019;
- CSE, "Representation, Availability and Gaps of Designated Groups by Occupational Groups," 2018;
- DND, "Employment Equity Workforce Analysis/Analyse de l'effectif liée à l'équité en matière d'emploi," March 2018;
- GAC, "Employment Equity Workforce Analysis by occupational category, group and level as of September 30, 2017," 2018;
- ITAC, "ITAC – Designated Groups as of 2018-03-31," April 2019;
- PCO, "PCO Stats 1," 2018;
- Public Safety Canada, "Workforce Representation and Workforce Availability for Employment Equity Groups by Classification Group, Public Safety Canada, September 30, 2017," 2018; and
- RCMP, *RCMP Employment Equity Annual Report 2017–2018*, undated.

[46] DND, DND/CAF Response to NSICOP Questions on Fact Checking, July 17, 2019.

[47] See: DND/CAF, Defence Administrative Orders and Directives (DAOD) 5023-0, Universality of Service; and DND/CAF, *Canadian Armed Forces Employment Equity Report 2014–2015*, undated, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5023/5023-0-universality-of-service.html#int.

[48] RCMP, *RCMP Employment Equity Annual Report 2016–2017*, September 2017.

Gaps in representation per department or agency

34. As Table 1 demonstrates, representation rates for employment equity groups vary among departments and agencies within the security and intelligence community. This is also true for representation in more specific occupational groups, with different departments and agencies showing different strengths and weaknesses in representation for designated groups.

35. This section provides an overview of gaps in representation of designated groups identified by each department or agency and, where relevant, any concentration of designated group members in particular occupational groups or ranks as of 2017–2018.[49] The gaps in representation for each department and designated group, highlighted in red in organization-specific tables, range from large to relatively small. Gaps in this section are highlighted regardless of their size because of issues related to the accuracy of workforce availability estimates, which is discussed later in this section. The section also presents each department or agency's employment equity plan objectives and numerical goals.

[49] The departments and agencies under review provided NSICOP with employment equity data broken down by occupational categories and groups for fiscal years 2015–2016, 2016–2017 and 2017–2018. The data on the current representation of women, Aboriginal Peoples, members of visible minorities and persons with disabilities presented in the following tables are for fiscal year 2017–2018.

Canadian Armed Forces

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	LMA	Current	LMA	Current	LMA	Current	LMA	Current
Overall	14.5%	15.0%	3.4%	2.8%	6.0%	7.2%	n/a	n/a
Executive level	n/a	7.2%	n/a	0.9%	n/a	2.0%	n/a	n/a

Source: Data retrieved from CAF, *Employment Equity Report 2017–2018*, undated.

Notes:
- Includes regular force members only
- The CAF is not required to set employment equity goals for persons with disabilities due to operational requirements and the principle of the Universality of Service, which requires that CAF members be "physically fit, employable and deployable for general operational duties."[50]

Table 2: Representation of Designated Groups in the Canadian Armed Forces

- Aboriginal peoples are underrepresented in the CAF in almost all military occupational groups, with the highest representation in officer cadet positions (5.9%).
- The overall representation of women is above LMA among officers in the regular force. Women are represented above LMA in medical and dental (47.5%), and support positions (35.8%). Women are underrepresented in combat arms (4.9%) and air operations pilot (5.1%) positions.
- Representation of designated groups is highest at lower ranks among officers in the regular force, with the highest representation of members of visible minorities at the Second Lieutenant rank (19.1%), and the highest representation of women (24.2%) and Aboriginal peoples (2.7%) at the Lieutenant rank.
- Among the military personnel of the Canadian Forces Intelligence Command (CFINTCOM), representation of women is 14.4%, of Aboriginal peoples is 3.2% and of members of visible minorities is 7%.
- The representation of women at CFINTCOM is lower than their overall representation in the CAF and has decreased from 17.1% in 2015.[51]

36. The CAF's *Employment Equity Plan 2015–2020* has a timeline of five years and the overarching goal of "achieving a representative military force that Canadians rightly expect from their military leadership."[52] The plan sets long-term numerical goals to increase the overall representation of each designated group over 10 years, specifically: 25.1% representation of women, 3.5% representation of

[50] See: DND/CAF, *Defence Administrative Orders and Directives (DAOD) 5023-0, Universality of Service*, undated; and DND/CAF, *Canadian Armed Forces Employment Equity Report 2014–2015*, undated, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5023/5023-0-universality-of-service.html#int.

[51] In 2015, representation of women military personnel in CFINTCOM was 17%. DND/CAF, Canadian Armed Forces Employment Equity Designated Group Membership CFINTCOM March 2015 to March 2018, 22 January 2019.

[52] DND/CAF, *Canadian Armed Forces Employment Equity Plan 2015–2020,* undated.

Aboriginal peoples and 11.8% representation for members of visible minorities by 2026.[53] To meet this goal, the plan lists several initiatives, including to recruit diverse applicants in the CAF; foster an inclusive and equitable workplace; support career progression for designated group members; provide employment equity and diversity training; and ensure accountability for the implementation of employment equity initiatives.[54]

[53] The CAF is not required to set employment equity goals for persons with disabilities due to operational requirements and the principle of the Universality of Service, which requires that CAF members be "physically fit, employable and deployable for general operational duties." See: DND/CAF, *Defence Administrative Orders and Directives (DAOD) 5023-0, Universality of Service*, undated; and DND/CAF, *Canadian Armed Forces Employment Equity Report 2014–2015*, undated, https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/5000-series/5023/5023-0-universality-of-service.html#int.

[54] DND/CAF, *Canadian Armed Forces Employment Equity Plan 2015–2020,* undated.

Canada Border Services Agency

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	44.4%	47.5%	4.1%	3.3%	11.9%	14.7%	4.4%	3.4%
Executive level	45.5%	37.1%	5.9%	2.4%	8.5%	8.4%	2.3%	2.7%

Source: Data retrieved from CBSA, "Employment Equity Data (April 2015-October 2018)," October 2018.

Table 3: Representation of Designated Groups in the Canada Border Services Agency

- Aboriginal peoples and persons with disabilities are underrepresented at CBSA. Both groups are underrepresented in operational occupations, specifically in border services officer positions.
- Women and Aboriginal peoples are underrepresented in executive positions.

37. CBSA's *Employment Equity Action Plan 2016–2019* has a timeline of three years and outlines four broad objectives: to renew the workforce by addressing gaps in representation and skills shortages; to increase awareness and understanding of diversity and inclusion; to create an inclusive culture; and to ensure leaders are accountable for fostering a healthy and inclusive environment.[55] CBSA's goal is to narrow the representation gaps for designated groups across the organization and within all occupational groups.

[55] Canada Border Services Agency (CBSA), *Employment Equity Action Plan 2016–2019*, undated.

Canadian Security Intelligence Service

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	47.3%	48.5%	2.6%	2.3%	18.5%	16.5%	4.6%	4.2%
Executive level	47.3%	40.0%	2.6%	2.0%	18.5%	7.0%	4.6%	3.0%

Source: Data retrieved from CSIS, "Designated Groups as of 2018-03-31," January 2019.

Table 4: Representation of Designated Groups in the Canadian Security Intelligence Service

- Aboriginal peoples, members of visible minorities and persons with disabilities are underrepresented at CSIS.
- Women remain underrepresented in executive positions.
- Representation of members of visible minorities is below their estimated WFA in executive, middle manager and professional positions. Representation of Aboriginal peoples is below their estimated WFA in executive and administrative positions.
- Representation of persons with disabilities is below their estimated WFA in executive and professional positions.

38. CSIS's *Triennial Employment Equity Plan 2017–2020* has a timeline of three years and outlines several initiatives to reduce employment barriers for members of designated groups. The initiatives include: identifying any systemic barriers in the agency's policies and practices; increasing representation of designated group members in senior and middle management; facilitating the hiring, promotion and retention of designated group members; increasing the representation of persons with disabilities, members of visible minorities and Aboriginal peoples; raising awareness of the agency's duty to accommodate; and implementing anti-harassment training.[56]

39. CSIS's short-term objectives are the full representation of women and persons with disabilities in senior manager positions and the full representation of Aboriginal peoples and persons with disabilities in middle and other management positions by 2020. In the same period, CSIS plans to reduce the gap by 50% for members of visible minorities in middle and other manager positions; reduce the gap by 50% for persons with disabilities in professional positions; and reduce the gap by 30% for members of visible minorities in professional positions.[57]

[56] CSIS, *Triennial Employment Equity Plan 2017–2020*, undated.
[57] CSIS, *Triennial Employment Equity Plan 2017–2020*, undated.

Communications Security Establishment

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	36.7%	37.3%	1.8%	2.0%	21.5%	11.4%	4.2%	3.7%
Executive level	27.6%	30.4%	2.5%	4.3%	8.6%	4.3%	5.9%	0.0%

Source: Data retrieved from CSE, "Representation, Availability and Gaps of Designated Groups by Occupational Groups," 2018.

Table 5: Representation of Designated Groups in the Communications Security Establishment

- Members of visible minorities and persons with disabilities are underrepresented at CSE.
- Representation of members of visible minorities is below their estimated WFA in senior and middle management positions, and in professional positions.
- Representation of persons with disabilities is below their estimated WFA in management, professional and supervisor positions.
- Of the 37.3% of women at CSE, approximately half work in a corporate function.[58]
- It is also noteworthy that the representation of women is below WFA estimates in middle manager and supervisor positions.

40. CSE's *Employment Equity Action Plan 2017–2020* has a timeline of three years and outlines a number of initiatives based on recommendations from an employment systems review conducted in 2016.[59] One of the initiatives listed is to "develop an employment equity plan in compliance with the *Employment Equity Act* requirements."[60] In its 2017–2020 plan, CSE does not establish short-term or long-term numerical goals for representation of designated groups overall or within each occupational category and group.

[58] CSE, International Women's Day – Journée Internationale de la femme, March 2018.
[59] CSE, *Employment Equity Action Plan 2017–2020*, November 2018.
[60] CSE, *Employment Equity Action Plan 2017–2020*, November 2018.

Department of National Defence

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	39.5%	40.0%	2.6%	3.1%	8.7%	7.8%	4.6%	5.4%
Executive level	43.5%	42.4%	3.5%	<5	11.2%	4.1%	2.4%	5.9%

Source: Data retrieved from DND, "Employment Equity Workforce Analysis / Analyse de l'effectif liée à l'équité en matière d'emploi," March 2018.

Table 6: Representation of Designated Groups in the Department of National Defence

- Visible minorities are underrepresented at DND. Per occupational group, members of visible minorities are underrepresented in management, professional and scientific, technical, and operational positions.
- For the civilian intelligence personnel of CFINTCOM, the representation of women is 37.1%, of Aboriginal peoples is 2.4%, of members of visible minorities is 9% and of persons with disabilities is 6.9%.
- Within CFINTCOM, women are represented below their WFA of 44.9%. Women are underrepresented in management, scientific and professional, administrative and foreign service, technical, and administrative support positions.

41. DND's *Civilian Employment Equity Plan 2014–2017* has a timeline of three years and lays out the four main pillars of its employment equity goals and initiatives: a representative workforce; an inclusive workplace; leadership and accountability; and meaningful communication and consultation.[61] The objectives associated with each pillar include: increasing representation of designated groups through recruitment; eliminating barriers within staffing processes; supporting the career advancement of designated group members; sensitizing managers, supervisors and employees to the importance of a diverse and inclusive workplace; and helping senior management foster a respectful and inclusive workplace culture.

42. DND's goal is to close the representation gap for designated groups across the organization and within the operational categories.[62] DND's *Civilian Employment Equity Plan 2014–2017* expired in 2017 and the department has not finalized its updated plan.

[61] DND/CAF, *Civilian Employment Equity Plan 2014–2017*, undated.
[62] DND/CAF, *Civilian Employment Equity Plan 2014–2017*, undated.

Global Affairs Canada

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	57.6%	55.3%	3.1%	4.6%	13.9%	20.3%	3.9%	3.6%
Executive level	51.4%	42.5%	5.0%	4.0%	9.5%	11.9%	2.3%	3%

Source: Data retrieved from GAC, "Employment Equity Workforce Analysis by occupational category, group and level as of September 30, 2017," 2018.

Table 7: Representation of Designated Groups in Global Affairs Canada

- Women and persons with disabilities are underrepresented at GAC.
- Women are underrepresented in executive, administrative and especially foreign service positions, as well as in technical, operational and administrative support positions.
- Persons with disabilities are underrepresented in administrative and foreign service and in scientific and professional positions.

43. GAC's *Employment Equity Action Plan 2018–2021* has a timeline of three years and establishes two primary objectives: to develop a corporate culture that promotes inclusion and addresses systemic or attitudinal barriers to employment for designated group members; and to eliminate gaps in representation for designated group members overall and within occupational categories and groups.[63]

44. The department's long-term goal is to achieve full representation and equitable distribution of designated group members across the organization. Its short-term numerical goals are to close representation gaps for designated group members by occupational category. Specific recruitment goals are set at 65% for women in foreign service positions and 40% for women in computer science positions by 2021.

[63] Global Affairs Canada (GAC), *Employment Equity Action Plan 2018–2021*, undated.

Integrated Terrorism Assessment Centre

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	47.3%	68.0%	2.6%	5.0%	18.5%	13%	4.6%	5.0%
Executive level	47.3%	67.0%	2.6%	0.0%	18.5%	0.0%	4.6%	0.0%

Source: Data retrieved from ITAC, "ITAC – Designated Groups as of 2018-03-31 (Excl. Students)," April 8, 2019.

Table 8: Representation of Designated Groups in the Integrated Terrorism Assessment Centre

- Aboriginal peoples, members of visible minorities and persons with disabilities are underrepresented in ITAC's permanent complement, particularly at executive levels.

45. It is important to note that 40% of ITAC employees are secondments from other organizations in the security and intelligence community. The percentages listed in the above chart include permanent ITAC and seconded CSIS employees only. The inclusion of other seconded employees would show a higher representation of women and visible minorities across the organization and in executive positions.[64] In addition, ITAC falls under CSIS's human resources management framework. CSIS provides ITAC with corporate support and ITAC employees are hired as CSIS employees.[65] For the purposes of this review, all CSIS policies and initiatives on diversity and inclusion apply to ITAC staff.

[64] ITAC, ITAC Submission for NSICOP Review: Diversity and Inclusion in the Security and Intelligence Community, April 10, 2019.
[65] ITAC, ITAC Submission for NSICOP Review: Diversity and Inclusion in the Security and Intelligence Community, January 25, 2019.

Privy Council Office

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	52.2%	57.3%	1.8%	2.9%	12.7%	13.0%	4.0%	3.4%
Executive level	47.1%	52.3%	n/a	0.0%	9.2%	4.5%	2.3%	4.5%

Source: Data retrieved from PCO, "PCO Stats 1," 2018.

Table 9: Representation of Designated Groups in the Privy Council Office

- Persons with disabilities are underrepresented in scientific and professional, technical, and administrative support positions at PCO.
- Members of visible minorities are underrepresented in executive positions, and in certain scientific and professional and certain technical positions at PCO.
- In PCO's National Security and Intelligence Advisor branch, the representation of women is 45.0%, of Aboriginal peoples is 2.7%, of members of visible minorities is 16.2% and of persons with disabilities is 5.4%.

46. PCO's *Employment Equity and Diversity Plan 2016–2019* focuses on five guiding principles: improving the representation of designated groups where underrepresentation exists; increasing accountability through leadership; supporting accommodation needs of all employees; sustaining an organizational culture that embraces diversity; and respecting statutory requirements.[66] In its 2016–2019 plan, PCO does not establish short-term or long-term numerical goals for representation of designated groups overall or within each occupational category and group.

[66] PCO, *Employment Equity and Diversity Plan 2016–2019*, undated.

Public Safety Canada

	Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
	WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	55.3%	61.1%	3.1%	4.2%	15.1%	11.0%	3.9%	5.9%
Executive level	46.3%	54.9%	6.6%	8.5%	7.5%	7.0%	2.3%	2.8%

Source: Data retrieved from Public Safety Canada, "Workforce Representation and Workforce Availability for Employment Equity Groups by Classification Group, Public Safety Canada, September 30, 2017," 2018.

Table 10: Representation of Designated Groups in Public Safety Canada

- Over the past five years, Public Safety Canada has closed representation gaps for women, Aboriginal peoples and persons with disabilities in almost all occupational groups.[67]
- Members of visible minorities are underrepresented in executive, scientific and professional, and administrative and foreign service positions at Public Safety Canada.

47. Public Safety Canada's *2016–2019 Diversity and Employment Equity Action Plan* has a timeline of three years and lists three overarching objectives: to ensure management promotes an organizational culture that values diversity and inclusion; to increase recruitment of members of designated groups, specifically members of visible minorities; and to establish and maintain a respectful and inclusive workplace.[68] The department's goal is to close the representation gap for members of visible minorities across the organization and within occupational groups. Public Safety Canada is currently finalizing its employment equity plan for 2019–2022.

[67] Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.
[68] Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.

Royal Canadian Mounted Police

		Women		Aboriginal Peoples		Members of Visible Minorities		Persons with Disabilities	
		WFA	Current	WFA	Current	WFA	Current	WFA	Current
Overall	All	48.0%	39.5%	4.0%	6.8%	18.0%	12.0%	5.0%	2.4%
By Personnel group	RM[69]	49.3%	21.6%	3.1%	7.8%	15.1%	11.1%	n/a	1.7%
	CM	48.0%	51.7%	4.0%	3.9%	18.0%	13.6%	5.0%	2.7%
	PSE	48.0%	77.6%	4.0%	5.7%	18.0%	13.7%	5.0%	4.1%
Executive level	RM	52.1%	21.8%	2.8%	8.4%	12.7%	5.8%	n/a	0.7%
	CM	52.1%	56.4%	2.8%	1.7%	12.7%	7.7%	2.8%	0.9%
	PSE								

Source: Data retrieved from RCMP, *RCMP Employment Equity Annual Report 2017–2018*, undated.

Note: Due to operational requirements, the RCMP is not required to set employment equity goals for persons with disabilities for the RM category.[70]

Table 11: Representation of Designated Groups in the Royal Canadian Mounted Police

- Regular Members (RM) represent 62% of the RCMP's total workforce and constitute the organization's sworn police officer cadre.[71]
    - Women and members of visible minorities are underrepresented among Regular Members, particularly in senior leadership positions.
- Civilian members (CM) of the RCMP are recognized under the *Royal Canadian Mounted Police Act* and represent 12% of the total workforce.[72] In May 2020, civilian members not appointed to a rank will be deemed employees under the *Public Service Employment Act*.
    - Members of visible minorities, Aboriginal peoples and persons with disabilities are underrepresented among civilian members.
- Public service employees (PSE) at the RCMP are recognized under the *Public Service Employment Act* and represent 26% of the total workforce.[73]
    - Members of visible minorities and persons with disabilities are underrepresented among public service employees. Representation of both groups is below their estimated WFA in economics and social sciences positions and financial administration positions.

[69] Representation rates for designated groups among regular members of the RCMP are compared with LMA instead of WFA.
[70] RCMP, *RCMP Employment Equity Annual Report 2016–2017*, September 2017.
[71] RCMP, *RCMP Employment Equity Annual Report 2017-2018*, undated.
[72] RCMP, *RCMP Employment Equity Annual Report 2017-2018*, undated.
[73] RCMP, *RCMP Employment Equity Annual Report 2017-2018*, undated.

- Although the representation of women is above WFA estimates, it is noteworthy that women make up a large proportion of the workforce in administrative (80.6%) and clerical (88.4%) positions.
- The highest representation of Aboriginal peoples and persons with disabilities are also in administrative and clerical positions.

48. The RCMP's 2013 *Gender and Respect: The RCMP Action Plan* had a timeline of three years and focused key actions and targets on the organization's Regular Members (police officers). For Regular Members, the RCMP set long-term numerical goals to increase the overall representation of women to 30%, of Aboriginal peoples to 10% and of members of visible minorities to 20% by 2025.[74] The action plan did not set representation targets for the organization's civilian or public service employee workforce.

49. The plan outlined several objectives related to improving workplace culture and representation. The objectives include addressing harassment; ensuring transparency and objectivity in promotions; increasing recruitment of women and members of other designated groups; improving the application process; ensuring a representative officer cadre; and retaining Regular Members.[75]

50. The RCMP's *Gender and Respect* Action *Plan* concluded in 2016–2017 and the agency is currently preparing a new version of its employment equity plan.[76]

---

[74] RCMP, *RCMP Employment Equity Annual Report 2017-2018*, undated.
[75] RCMP, *Gender and Respect: the RCMP Action Plan*, undated.
[76] RCMP presentation, Refreshing the Employment Equity Planning Process, May 2018.

Comparisons

51. This section provides a broader context by explaining how representation of designated groups in the security and intelligence community compares with the public service average, and highlighting the strengths and weaknesses in representation across the organizations under review.

Comparison with the public service average ↓

52. The representation of members of designated groups is *lower than* the federal public service average in a majority of the organizations in the security and intelligence community.[77]

Comparison of underrepresented groups within the security and intelligence community ↔

53. In general, organizations across the security and intelligence community show steady or slightly increasing representation of members of designated groups over the past three years.[78] Current figures show that:

- the representation of **women** and **Aboriginal peoples** is *higher than* their estimated availability in a majority of the organizations under review; and
- the representation of **members of visible minorities** and **persons with disabilities** is *lower than* their estimated availability in a majority of the organizations under review.

Comparison of designated groups at executive levels ↓

54. A useful point of comparison for representation of designated groups is at the executive level, as the skills and experience required are transferable. Current figures show that:

- the representation of **women** and **members of visible minorities** is *lower than* their estimated availability at executive levels in a majority of the organizations under review;[79]
- the representation of **persons with disabilities** is *higher than* their estimated availability at executive levels in a majority of the organizations under review; and
- there is currently not enough information on the representation of **Aboriginal peoples** at executive levels within the security and intelligence community to assess their representation.

---

[77] The departments and agencies under review provided employment equity data to the Committee for fiscal years 2015–2016, 2016–2017 and 2017–2018. The representation rates listed are from fiscal year 2017–2018.

[78] The departments and agencies under review provided employment equity data to the Committee for fiscal years 2015–2016, 2016–2017 and 2017–2018.

[79] The departments and agencies under review provided employment equity data broken down by occupation categories and groups to the NSICOP Secretariat for fiscal years 2015–2016, 2016–2017 and 2017–2018.

Challenges

55. The data behind the representation gaps presented in the preceding charts has limitations that potentially affect its reliability. This section describes two challenges, voluntary self-identification, and the accuracy of WFA and LMA estimates, as well as a possible limitation in data collection.

Self-identification

56. Self-identification is a necessary and important step in creating an inclusive workforce. Under the *Employment Equity Act*, persons must self-identify to be counted as part of a designated group. However, identifying as a visible minority, an Aboriginal person or a person with a disability is voluntary. The Canadian Human Rights Commission auditing criteria requires an 80% rate of return for self-identification forms for departments and agencies in the federal public service.[80] Importantly, the return rate represents the percentage of employees who have returned the form, not necessarily those who have responded to the voluntary portion of the form in which employees self-identify.[81] Departments use self-identification information primarily to assess the representation of designated groups across the organization.[82] The information ensures that employers have the necessary data to prepare an employment equity plan or address those barriers faced by people in designated groups. Self-identification information is confidential and does not appear on personnel files. The issue of self-identification may affect any organization in the government. Of the organizations under review, the CAF, CSIS, ITAC, CSE, GAC, PCO and the RCMP have return rates above the 80% requirements. Falling below this threshold are CBSA with 64.9%, DND with 78.1% and Public Safety Canada with 73%. Nonetheless, the data in this report illustrate trends in representation of designated groups across the organizations under review.

57. CBSA, CSE, DND, GAC, PCO and Public Safety Canada have identified individuals' reluctance to self-identify as a member of a designated group as an obstacle to assessing the composition of their workforce and their recruiting pool. For example, GAC found that persons with disabilities often do not self-identify due to the "fear of being labeled as a person with disabilities and not being recognized for actual competencies."[83] Similarly, DND's 2010 employment systems review found that employees were concerned about "personal repercussions associated with self-identification."[84] From a recruitment perspective, employment systems reviews for PCO and CSE found that managers did not receive self-identification information for qualified candidates, which hindered their ability to close representation gaps.[85]

---

[80] Written communication from the Canadian Human Rights Commission, May 31, 2019.
[81] Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.
[82] For more information, see: Public Service Commission, "Self-Declaration Information," www.canada.ca/en/public-service-commission/services/appointment-framework/employment-equity-diversity/self-declaration-information.html.
[83] GAC, Notes from the meetings between Leslie Norton and Global Affairs Canada Employment Equity Network Representatives, August 15–18 and 28–29, and September 7 and 22, 2017.
[84] Sylvie C. Lalonde, *The 2009–2010 Department of National Defence Employment Systems Review: Workforce Component,* Civilian Personnel Research and Analysis, Personnel and Family Support Research, DND/CAF, July 2011.
[85] Linda Buchanan, "Employment Systems Review Report: Privy Council Office," *HDP Group*, March 30, 2015.

58. Self-identification campaigns and internal communications are ways organizations try to increase awareness on these issues. CBSA, CSIS, CSE and DND conducted campaigns to demystify the self-identification process and encourage employees to self-identify.[86] In 2016, CSIS began publishing a newsletter entitled "Our Diversity Climate," which aims to communicate to employees the value of diversity. CSE's initiatives include the "Inside Cover" and "Humans of CSE" that seeks to highlight the diversity inside the organization. While departments and agencies have made efforts to encourage employees to self-identify, employees' reluctance to do so may be indicative of larger systemic and attitudinal barriers faced by designated group members in the security and intelligence community.[87]

Workforce availability and labour market availability

59. WFA and LMA estimates are the benchmarks organizations use to determine whether designated groups are underrepresented in their workforce. TBS, Employment and Social Development Canada (ESDC) and Statistics Canada determine WFA and LMA estimates for occupational groups in departments across the public service. TBS provides job category definitions to ESDC; this organization uses data from the most recent census and the Canadian Survey on Disability related to individuals' field of study and previous work experience to calculate the estimated availability of designated groups for each occupational group in the Canadian workforce.[88]

60. The 2017 report of the Joint Union/Management Task Force on Diversity and Inclusion identified several issues with WFA estimates that also apply to LMA estimates. Two are of particular importance. The first issue is that current representation rates are calculated using data from the 2011 census. Organizations use those calculations to determine their employment equity objectives, recruitment strategies and hiring decisions. However, that data always reflects a point in time: it does not account for the historically consistent rates of growth among some designated groups as a share of Canada's population, notably members of visible minorities and Aboriginal peoples.[89] In short, calculations of availability and goals for hiring quickly become outdated. This problem is compounded by the second issue, which is that most government organizations use availability estimates as a 'ceiling' and not as a 'floor' (i.e., as a goal to achieve rather than to surpass).[90] This is true of the majority of the security and intelligence organizations under review, which have set as their employment equity goals the closing of gaps in representation of various designated groups. Together, these two issues result in a public

---

[86] The campaigns seek to explain the purpose of self-identification and clarify the confidentiality of the data provided. See for example, DND, YOU have the ANSWER, undated; and CSIS, Self-identification: Employment Equity Program, February 23, 2018.
[87] NSICOP Secretariat consultation with TBS, Acting Manager Employment Equity, Diversity and Inclusion, Office of the Chief Human Resources Officer, February 5, 2019.
[88] NSICOP Secretariat consultation with TBS, Acting Manager of Employment Equity, Diversity and inclusion, Office of the Chief Human Resources Officer, February 5, 2019.
[89] For example, members of visible minorities as a share of Canada's population grew from 16.2% in 2006 to 22.3% in 2016. See: Catalyst, "Quick Take: Visible Minorities in Canada," April 9, 2018, https://www.catalyst.org/research/visible-minorities-in-canada/.
[90] NSICOP Secretariat consultation with TBS, Acting Manager Employment Equity, Diversity and Inclusion, Office of the Chief Human Resources Officer, February 5, 2019.

service, and a security and intelligence community, where the representation of designated groups continually lags behind actual population demographics.

61. The Committee's review of WFA and LMA estimates across the organizations under review also raised questions about the methodology for determining availability. Specifically, CBSA and DND have WFA estimates of 0% for several designated groups in certain occupational categories. With a WFA estimate of 0%, the department or agency may not consider the absence of representation as a gap they need to address. In the case of DND, for example, at least 20 out of 50 different positions in the operational occupational category have a WFA of 0% for women, members of visible minorities and Aboriginal peoples.

Data collection

62. The *Employment Equity Act* does not require organizations to collect data disaggregated by sex for each designated group. That said, the information provided by the CAF disaggregated its employment equity data by sex, which revealed low representation of visible minority and Aboriginal women compared with men in those designated groups in almost all occupational categories.[91] The CAF's more granular breakdown provided a clearer picture of the representation of women across the organization and informed the organization's employment equity planning.[92]

63. This limitation will soon be addressed for all government organizations. In May 2019, the Minister of Innovation, Science and Economic Development announced the launch of Statistics Canada's Centre for Gender, Diversity and Inclusion Statistics. The government:

> intends to address gaps in gathering data and to better use data related to gender and diversity. This includes proposing $6.7 million over five years, starting in 2018–19, and $0.6 million per year ongoing, for Statistics Canada to create a new Centre for Gender, Diversity and Inclusion Statistics. . . .
>
> The Centre will work to address gaps in the availability of disaggregated data on gender, race and other intersecting identities to enrich our understanding of social, economic, financial and environmental issues. The work conducted at the Centre will include collecting, analyzing and disseminating data on visible minorities to understand the barriers [that] different groups face and how best to support them with evidence-based policy.[93]

---

[91] DND/CAF, *CAF Employment Equity Report 2017–2018*, undated, Annex A, Schedule 3.
[92] DND/CAF, *CAF Employment Equity Report 2017–2018*, undated.
[93] Canada, *Budget 2018*.

Organizational efforts to promote diversity and foster inclusion

64. The first half of this chapter provided an overview of employment equity requirements and the state of diversity in the security and intelligence community as of 2017–2018. The rest of this chapter goes beyond employment equity obligations and assesses efforts by those organizations under review to promote diversity and to foster inclusion across their workforces.

Promoting diversity

65. This section describes the efforts of security and intelligence organizations to promote diversity. It evaluates the important role that leadership plays in these efforts, and corporate efforts to achieve organizational buy-in; analyze and understand the workforce; and recruit and hire members of diverse groups.

Leadership and accountability

66. Organizational leadership and corporate policies play a critical role in promoting and enabling diversity.[94] CSIS's 2010 Diversity Roadmap states, "Sustainable diversity and inclusion requires visible commitment from the leaders of the organization."[95] Leaders of all organizations under review recognize diversity and inclusion as vital to the success of their organizations. One of the most visible expressions of organizational leadership is the appointment of 'champions.'[96] All of the organizations under review have appointed senior-level champions to act as spokespersons and advocates for different groups or initiatives. Champions have been appointed for all four designated groups and the LGBTQ2+ community, and for broader initiatives, including Champions for Diversity and Inclusion, GBA+, and Women, Peace and Security.[97]

---

[94] See: Juliet Bourke and Bernadette Dillon, "The Diversity and Inclusion Revolution," *Deloitte Review*, Issue 22, January 2018; Ilene Wasserman, et. al., "Dancing with Resistance: Leadership Challenges in fostering a Culture of Inclusion," 2008, https://www.researchgate.net/publication/235007850_Dancing_with_resistance_Leadership_challenges_in_fostering_a_culture_of_inclusion; and Matt Krentz, "Survey: What Diversity and Inclusion Policies Do Employees Actually Want?" *Harvard Business Review*, February 5, 2019.

[95] Judy Laws and Denise McLean, "Public Safety and Emergency Preparedness Canada (PSEPC) Diversity Roadmap Project," *Graybridge Malkam*, June 15, 2010.

[96] The 2017 U.S. Intelligence Community report noted the important role leaders play in increasing the visibility of managers and employees of diverse backgrounds as it can "positively impact the way people think" by "providing positive, diverse role models in positions of leadership." See IC Equal Employment Opportunity and Diversity Office, "Diversity and Inclusion: Examining Workforce Concerns within the Intelligence Community," January 2017, https://fas.org/irp/dni/diversity.pdf; and Katherine W. Phillips, "How Diversity Makes Us Smarter," *Scientific American*, October 1, 2014, https://www.scientificamerican.com/article/how-diversity-makes-us-smarter/.

[97] DND/CAF, Appointment of Defence Champions/Nomination des champions de la défense, CANFORGEN 074/18 CDS 008/18 261846Z, April 2018.

67. Another expression of organizational leadership is the extent to which responsibility for diversity is spread across an organization.[98] As the 2018 employment systems review of Public Safety Canada noted, efforts to promote diversity and inclusion were "undermined by the treatment of employment equity as a separate program rather than a lens through which barriers to [designated] groups have been systematically identified and measures put in place to create a representative workforce and an inclusive workplace."[99] In many of the organizations under review, diversity and inclusion are the sole responsibility of the human resources department, and not integrated across levels of the organization. For example, PCO's 2015 employment systems review found that employment equity goals were established by the human resources division as a "stand alone program."[100] Managers were not involved in the development of plans or strategies to achieve these goals; this practice, according to the PCO review, "undermines managerial accountability for creating a representative workforce and an inclusive workplace."[101] By contrast, the RCMP created a Workforce Culture and Employee Engagement Unit in 2016 responsible for promoting gender equality and culture change within the organization.[102] The head of this unit actively participates in regular discussions with senior leaders of the organization to promote diversity and inclusion throughout the organization.[103]

68. Ministers are responsible to the Prime Minister and ultimately to Canadians on their commitment to diversity and inclusion. In December 2016, the Prime Minister met with leaders of the security and intelligence community and officials from PCO and requested they establish a group of experts to address the specific challenges of diversity and inclusion in their organizations. In January 2017, the leaders of the CAF, the Canadian Coast Guard, CBSA, CSIS, CSE, DND and the RCMP established the "Security and Intelligence Diversity and Inclusion Tiger Team" with the stated aim of "exploring, advancing and implementing joint efforts to learn from one another and share best practices to enhance diversity and inclusion within and across [their] organizations through a variety of activities and initiatives."[104] The team met approximately every seven weeks and reported to the Deputy Secretary to the Cabinet (Results and Delivery) every six months. At the time of writing, the Tiger Team had not met since July 2018.[105] Tiger Team initiatives included joint recruitment initiatives, such as CSE's Young Professionals Network's Career Tradeshow, and joint engagement in the GBA+ Security and Defence Network.[106] Another Tiger Team initiative was the creation by the CAF, CBSA, the Coast Guard and the

---

[98] Research by Deloitte identifies the integration of diversity and inclusion principles in all employee and business processes as an essential element of a diverse and inclusive organization. Juliet Bourke and Bernadette Dillon, "The Diversity and Inclusion Revolution," *Deloitte Review*, Issue 22, January 2018.

[99] Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.

[100] Linda Buchanan, "Employment Systems Review Report: Privy Council Office," *HDP Group*, March 30, 2015.

[101] Linda Buchanan, "Employment Systems Review Report: Privy Council Office," *HDP Group*, March 30, 2015.

[102] RCMP, Canada's National Action Plan on Women, Peace and Security 2017–2022: RCMP implementation plans, 2017.

[103] NSICOP Secretariat consultation with the RCMP, Director of the Workforce Culture and Employee Engagement Unit, April 5, 2019.

[104] Tiger Team Letter to Deputy Secretary to the Cabinet (Results and Delivery), January 2017.

[105] CSE, Written communication to NSICOP, July 23, 2019.

[106] Tiger Team Letters to Deputy Secretary to the Cabinet (Results and Delivery), January 2017 and March 2018.

RCMP of the Uniform Modernization Working Group to develop a more inclusive uniform design and procurement practice across the four organizations.[107]

69. The Committee noted several shortcomings with this initiative. First, the Tiger Team did not establish specific objectives for diversity and inclusion nor develop a performance measurement framework to assess the success of its initiatives.[108] Second, the representatives from each organization were all from human resources departments and organizations did not seek out members of employment equity groups for membership or participation on the Tiger Team. Organizations also did not always send the same representative to each meeting.[109] Third, the Tiger Team did not engage with designated groups within the security and intelligence community to inform their activities or initiatives. Finally, throughout its discussions, the Tiger Team focused on short-term initiatives without considering systemic challenges raised in various organization-specific studies or class-action lawsuits (the CAF and the RCMP), such as workplace culture and discrimination.[110]

70. Within departments and agencies, accountability for results is a cornerstone of public service leadership.[111] TBS policy requires performance management agreements for executive-level positions in every department and agency across the federal public service to include an indicator on diversity and inclusion.[112] Departments and agencies develop their own performance indicators based on the corporate priorities set by the Clerk of the Privy Council.[113] However, the majority of hiring and day-to-day employee management tasks are the responsibility of middle management.[114] Of the nine organizations under review, only two, CSIS and CSE, have incorporated a diversity and inclusion indicator for middle managers.[115] While laudable, their performance indicators lack specificity and measurable goals. At CSIS, for example, managers are assessed on their ability to promote "a healthy workplace."[116]

---

[107] Tiger Team Letter to Deputy Secretary to the Cabinet (Results and Delivery), March 2018; CBSA, Uniform Modernization Working Group Agenda, November 23, 2018.

[108] Of note, the Tiger Team attempted to measure diversity and inclusion in the security and intelligence community by proposing that four new questions be added to the Public Service Employee Survey. CSE reported that it is not aware of whether their proposed questions were included in the 2018 PSES. CSE written communication to NSICOP, June 13 and July 8, 2019.

[109] CSE, Written communication to NSICOP, July 8, 2019.

[110] NSICOP Secretariat consultation with former Chair of the Security and Intelligence Diversity and Inclusion Tiger Team, May 2, 2019.

[111] A report by Deloitte notes that measurable objectives for diversity and inclusion are only effective when important decision-makers are held accountable. It states "by taking accountability for goals, leaders signal the importance of diversity and inclusion as a business priority and help focus people's attention." Juliet Bourke and Bernadette Dillon, "The Diversity and Inclusion Revolution," *Deloitte Review*, Issue 22, January 2018.

[112] TBS, "MAF 2017 to 2018 people management methodology," https://www.canada.ca/en/treasury-board-secretariat/services/management-accountability-framework/maf-methodologies/maf-2017-2018-people-management-methodology.html

[113] By way of example, the 2019–2020 priorities focused on building and sustaining a healthy workplace, which includes taking action on harassment and discrimination, and fostering the inclusion of different voices and perspectives in governance and decision-making.

[114] NSICOP Secretariat consultation with TBS, Acting Manager Employment Equity, Diversity and Inclusion, Office of the Chief Human Resources Officer, February 5, 2019.

[115] NSICOP Secretariat consultation with CSIS, Representatives of the Health and Workplace Management Branch, April 8, 2019; and written communication from CSE, May 9, 2019.

[116] NSICOP Secretariat consultation with CSIS, Representatives of the Health and Workplace Management Branch, April 8, 2019.

At CSE, managers are assessed on their efforts to "create a workplace that is representative and inclusive by encouraging employee self-identification and participating in Diversity and Inclusion initiatives."[117]

71. The challenges of ensuring leadership accountability in the areas of diversity and inclusion are compounded by the absence of established ways of measuring organizational success or progress on diversity and inclusion in the public service. As the Joint Union/Management Task Force on Diversity and Inclusion noted, there is no government-wide framework and approach to diversity and inclusion, and that "without established goals, data and performance measures, it is difficult to determine progress and to know whether current initiatives, by themselves, will succeed in reducing or eliminating systemic barriers."[118] This is equally true for the security and intelligence community. Few of the organizations under review have established a performance assessment framework for their diversity and inclusion goals and initiatives, with three partial exceptions. In 2013–2014, CSIS created a "Diversity Scorecard" to measure its progress on employment equity, but stopped tracking progress in 2016 due to resourcing issues.[119] In its 2015–2020 employment equity plan, the CAF noted that it planned to develop a Performance Measurement and Evaluation Plan, but has not made progress in developing that plan.[120] As a final example, the Security and Intelligence Diversity and Inclusion Tiger Team stated in a letter to the Deputy Secretary to the Cabinet (Results and Delivery) in September 2017 an intention to "develop a [security and intelligence] community Performance Measurement Framework to track diversity issues;" this framework was not developed.[121]

Organizational buy-in

72. Research shows that while leadership commitment to diversity is important, ensuring that employees at all levels of the organization understand and accept the value of diversity is critical to the success of any initiatives, particularly at middle management levels.[122] However, misunderstandings about diversity and inclusion goals and even resistance to their implementation persist. As examples, the RCMP noted that resistance to diversity and inclusion initiatives was strongest at the Senior Non-Commissioned Officer level of the organization.[123] Similarly, the CAF's 2013 employment systems review identified continued resistance to the importance of diversity, including among senior leaders in the

---

[117] CSE, Written communication to NSICOP, May 9, 2019.

[118] TBS, *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017. https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/building-diverse-inclusive-public-service-final-report-joint-union-management-task-force-diversity-inclusion.html

[119] CSIS, Diversity Scorecard Tool, September 25, 2013.

[120] DND/CAF, Written communications, April 23, 2019.

[121] Security and Intelligence Tiger Team on Diversity and Inclusion, Annex B: Future plans for the S&I partners, September 2017; and NSICOP Secretariat consultation with former Chair of the Security and Intelligence Tiger Team on Diversity and Inclusion, May 3, 2019.

[122] See: Juliet Bourke and Bernadette Dillon, "The Diversity and Inclusion Revolution," *Deloitte Review*, Issue 22, January 2018; and Conference Board Business Diversity Council, "Middle managers: Engaging and enrolling the biggest roadblock to diversity and inclusion," *The Conference Board of Canada*, April 2007.

[123] NSICOP Secretariat consultation with the RCMP, Director of Workplace Culture and Employee Engagement Unit, April 5, 2019.

organization.[124] DND's most recent employment systems review found that "only the most senior executives are able to describe the organizational benefits of a more diverse workforce."[125] For its part, CSE's 2017 employment systems review revealed a "lack of visibility of employment equity/diversity and its recognition as a contributor to business results."[126]

73. Various organizations have implemented measures to better inform their members of the value and importance of diversity and inclusion. For example, in 2010 CSIS commissioned a report on the case for diversity and best practices to enhance diversity and inclusion in the organization.[127] This report stands out as a useful tool to both justify initiatives and implement strategies to improve diversity across CSIS. In a similar vein, the CAF developed a diversity strategy document to provide the "framework within which [it] will direct, promote and safeguard the respect and dignity of all persons as a core value within [its] institution."[128] DND and the CAF are also currently developing a joint civilian and military diversity action plan.[129]

74. Most organizations also offer employment equity and diversity training online. For their part, CSIS and CSE provide training on employment equity and diversity to employees during onboarding sessions.[130] CBSA employs a mandatory online course on diversity and race relations for all employees.[131] For the other organizations, these courses are voluntary and no organization makes career promotions conditional on the completion of courses on diversity or inclusion.[132]

Efforts to understand the workforce

75. The *Employment Equity Act* requires organizations to identify barriers to employment for designated groups and to institute policies and practices to address those barriers. This requires organizations to assess and understand their workforces. As noted earlier, the government renewed its commitment in 2015 to support the full implementation of GBA+, an analytical tool used across organizations in the federal public service to assess how different groups experience policies and

---

[124] Alla Skomorovsky and Sylvie Lalonde-Gaudreault, Canadian Armed Forces Employment Systems Review: Qualitative Component, Defence Research and Development Canada, Director General Military Personnel Research and Analysis, September 2013.
[125] Sylvie C. Lalonde, *The 2009–2010 Department of National Defence Employment Systems Review: Workforce Component,* Civilian Personnel Research and Analysis, Personnel and Family Support Research, DND/CAF, July 2011.
[126] Linda Buchanan, Employment Systems Review and *Employment Equity Act* Compliance Assessment: Communications Security Establishment, March 31, 2017.
[127] Judy Laws and Denise McLean, Public Safety and Emergency Preparedness Canada (PSEPC) Diversity Roadmap Project, *Graybridge Malkam*, June 15, 2010.
[128] DND/CAF, *Canadian Armed Forces Diversity Strategy*, 2016.
[129] DND/CAF, Written communication to NSICOP, April 25, 2019.
[130] NSICOP Secretariat consultation with CSIS, Representatives of the Health and Workplace Management Branch, April 8, 2019; and CSE, Written communication to NSICOP, May 9, 2019.
[131] CBSA, Learning Evaluation Data Summary Report Diversity and Race Relations H1000-P, July 18, 2018.
[132] It is noteworthy, however, that some research has demonstrated that diversity training can be ineffective in eliminating bias and sometimes triggers a backlash from employees. Frank Dobbin and Alexandra Kalev, "Why Diversity Programs Fail," *Harvard Business Review*, July–August 2016.

programs.[133] Like other departments, some security and intelligence organizations are using GBA+ to identify potential barriers in their recruitment, hiring and promotions.

76. The GBA+ assessment of staffing policies and practices at GAC and the RCMP stood out as best practices among the organizations under review. GAC's analysis sought to bring a GBA+ lens to all of its human resources and management policies and processes.[134] The RCMP's assessment recommended updating recruiting materials and reviewing mandatory requirements to ensure fair recruitment and hiring processes.[135] For its part, DND stated in a 2018 briefing to the Department for Women and Gender Equality that it had conducted a "complete institutional assessment: organization, doctrine, culture, to understand where to start, how to prioritize, and how to 'crack' both the organization at large . . . as well as the multiple areas and 'cultures' of work."[136] Despite repeated requests from the NSICOP Secretariat, DND failed to provide the Committee with documentation of its assessment.

77. There are other means used by organizations to understand the composition of their workforce and the potential barriers they face. Notable as a best practice, GAC and the RCMP conducted a 'clustering analysis' that, according to ESDC, is used "to determine whether a higher proportion of any designated group is found in the lower levels of occupational groups compared to non-designated counterparts."[137] The RCMP's analysis revealed important clusters of Aboriginal peoples and persons with disabilities in administrative and clerical positions, which informed their employment equity planning.[138] GAC's analysis found that women are clustered in lower levels in foreign service positions.[139] Internal research conducted by CSIS and GAC on barriers women face in executive and foreign service positions also stood out as a best practice.[140] The studies provided senior management with information about the systemic and attitudinal barriers to women's advancement in each organization and informed policies and initiatives to resolve the identified challenges.

78. In terms of members of visible minorities, DND and the CAF reported to the Minister of Canadian Heritage in its 2017–2018 annual multiculturalism report that the department was conducting an internal study on racism and discrimination. DND and the CAF stated in that report that data collection for this study was complete and that its "results provided important insights into these issues that inform/support organizational efforts to address them."[141] Despite repeated requests, DND failed to

---

[133] Canada, *Action Plan on Gender-based Analysis (2016–2020)*, 2016, https://cfc-swc.gc.ca/gba-acs/plan-action-2016-en.PDF.
[134] GAC, Guide to applying GBA+ using a Diversity and Inclusion Lens to Staffing, May 15, 2018.
[135] RCMP, GBA+ of Recruitment, June 2018.
[136] DND/CAF, Briefing to Status of Women Canada, November 2018.
[137] Canada, "Technical Guide *Employment Equity Act*," www.canada.ca/en/employment-social-development/services/employment-equity/tools/technical.html.
[138] RCMP, *RCMP Employment Equity Annual Report 2017–2018*, undated; and GAC, *Employment Equity Clustering Analysis Report Parts 1–3, 2017*. Cluster analyses are not required by government legislation or policy.
[139] GAC, *Employment Equity Clustering Analysis Report – Part III: Pooled (Rotational/Mobile) Workforce*, 2017.
[140] CSIS, Briefing note: Achieving Gender Equity at Senior Levels, March 8, 2016; and GAC, Women's Representation in the Foreign Service, August 2017.
[141] On 23 August 2019, DND stated that "the reference in the Annual Multiculturalism Report to the study's findings was incorrect," and the report "should have read 'will provide' instead of 'provided.'" DND/CAF, *The Joint Department of National Defence and Canadian Armed Forces Annual Multiculturalism Report – 2017/18*, undated.

provide the Committee with the results or any other documentation related to this study, including relevant studies that came to the attention of the Committee through media reports.[142]

Recruitment and hiring

79. Organizations need to recruit and hire diverse candidates to achieve a diverse workforce. Research demonstrates that this may require organizations to adjust their recruitment strategies to reach candidates of different genders, abilities, and racial or ethnocultural backgrounds, and to ensure that their hiring practices are free of bias.[143] As a practical example, CSIS's 2010 Diversity Roadmap identified establishing relationships in diverse communities, advertising and recruiting at colleges and universities, using specialized recruitment services, training people in cross-cultural interviewing skills, and reviewing recruitment processes for bias, as best practices for recruiting a diverse workforce.[144]

80. A majority of organizations reviewed have adopted proactive and targeted recruitment strategies to reduce representation gaps for all designated groups. CSIS and CSE were particularly notable for their collaboration with a number of agencies that specialize in the recruitment of persons with disabilities and women, and appointment of specialized diversity recruiters whose role is to reach out to ethnocultural community groups and student associations.[145] Another positive initiative is the Young Women in Public Safety Internship Program, launched by Public Safety Canada and its portfolio agencies, to increase recruitment of women.[146] CBSA is developing a three-year recruitment and retention strategy for Aboriginal peoples in border service officer positions.[147] Moreover, several organizations have made efforts to target members of designated groups in their staffing advertisements. CBSA, for

---

[142] For example, DND failed to provide a report by the Defence Aboriginal Advisory Group which noted that racism and discrimination "is a systemic issue." Dennis Ward, "Racism and discrimination 'rampant' throughout ranks and elements of Canadian Armed Forces says report," *APTN News*, January 19, 2017, https://aptnnews.ca/2017/01/19/racism-and-discrimination-rampant-throughout-ranks-and-elements-of-canadian-armed-forces-says-report/; DND also failed to provide a 2018 study tracking white supremacy and racism in the military from 2013 to 2018. Bryce Hoye, "Reservist suspected of neo-Nazi ties prompts questions about whether signals missed by military," *CBC News*, August 22, 2019, www.cbc.ca/news/canada/manitoba/neo-nazi-group-winnipeg-1.5253633.

[143] A research paper on diversity and inclusion in recruitment by a U.K. recruitment consulting firm noted that in order to recruit candidates of diverse backgrounds, organizations should implement targeted recruiting strategies, and review recruitment and hiring practices to ensure they are free of bias. Robert Walters, "Diversity and Inclusion in Recruitment," *Robert Walters Whitepaper*, 2017, www.robertwalters.co.uk/content/dam/robert-walters/country/united-kingdom/files/whitepapers/Diversity-In-Recruitment-Whitepaper-web.pdf.

[144] Judy Laws and Denise McLean, "Public Safety and Emergency Preparedness Canada (PSEPC) Diversity Roadmap Project," *Graybridge Malkam*, June 15, 2010.

[145] CSIS has a partnership with Lime Connect, an organization that supports the recruitment of persons with disabilities. See: CSIS, Renewal of Partnership with Lime Connect Canada for FY 2018-2019, 27 April 2018; and CSIS, *Diversity Recruitment – Proactive Marketing and Recruitment Work Plan 2019/20*, March 2019. CSE has engaged in initiatives to increase the participation of women in science, technology, engineering and math, including "Hackergal," "Women in Computing Canada," "Raspberry Pi" and "Technovation." CSE, *Communications Security Establishment Diversity and Inclusion Tile Work Plan 2018-2019*; and CSE, Written communication, May 9, 2019.

[146] Public Safety Canada, Young Women in Public Safety National Program July 2018, October 2018.

[147] However, an October 2018 audit of CBSA's Officer Induction Model found that, despite a need to increase representation of women and Aboriginal officers, "outreach and recruitment activities have not targeted these applicants in order to fill the gaps." See: CBSA, CBSA's Response to the MSR's Report on First Nations Border Crossing Issues (Near Term Measures), September 2018; and CBSA, *Internal Audit and Program Evaluation Directorate: Evaluation of the Officer Induction Model*, October 2018.

example, advertised several positions for persons who self-identify as Aboriginal peoples, persons with disabilities or as a member of a visible minority.[148] Similarly, CSIS and PCO have both encouraged hiring managers to obtain information on targeting designated groups in staffing advertisements.[149]

81. GAC and the RCMP both conducted GBA+ reviews of their recruitment or hiring processes to ensure they are bias-free.[150] GAC's "Guide to applying GBA+ using a Diversity and Inclusion Lens to Staffing" aimed to "replenish or refresh the staffing being carried out in a manner that adheres to the GBA+ philosophy thus leading to a diverse and inclusive workplace and workforce."[151] The RCMP's review of recruitment processes sought to identify the barriers facing diverse applicants throughout different phases of the recruitment and hiring process.[152] In terms of bias-free hiring practices, CBSA and GAC stood out in terms of ensuring adequate representation of designated group members on selection boards and bias-free training requirements for interviewers.[153]

The Committee's assessment of organizational efforts to promote diversity

82. The leadership of the security and intelligence community recognizes the importance of a diverse workforce and some organizations have made efforts to promote and increase diversity in their workforce. However, accountability for diversity and inclusion at executive and managerial levels is limited and organizations have not developed a performance measurement framework to measure their progress. Responsibility for diversity and inclusion tends to be concentrated in human resources areas, rather than spread across the organization, including among middle-managers who make the majority of hiring decisions. Outside of specific organizational contexts, leadership at the level of the security and intelligence community (the Tiger Team) suffers from notable weaknesses, including a lack of diversity among its own membership and a focus on short-term measures. Finally, while organizations have implemented measures to increase representation of designated groups through recruitment, few have made efforts to better understand barriers facing designated groups in their workforce or review internal policies for bias.

---

[148] CBSA, Selection process number: 2018-IA-HRB-EX-1-229, November 2018. Public Safety's 2018 employment systems review noted "restricting staffing processes to only members of an employment equity group in order to close gaps in under-represented is not recommended. One the one hand, feedback over the years from Employment Equity and Diversity Committees indicate that members of employment equity groups want to be hired on the basis of their skills and knowledge not on the basis of their membership in a group." Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.

[149] PCO, Employment Equity Staffing Options, February 2018; and CSIS, Diversity Hiring Communique, June 14, 2015.

[150] Intergage Consulting Group Inc., Guide to applying GBA+ using a Diversity and Inclusion Lens to Staffing, GAC, May 15, 2018; and RCMP, GBA+ of Recruitment, June 2018.

[151] Intergage Consulting Group Inc., Guide to applying GBA+ using a Diversity and Inclusion Lens to Staffing, GAC, May 15, 2018.

[152] RCMP, GBA+ of Recruitment, June 2018.

[153] CBSA, CBSA Inventory of Assessment Board Members of Employment Equity Designated Groups, August 2018; and GAC, Diversity & Inclusion (D&I) Presentation to Executive Board, May 2018.

Fostering inclusion

83. According to TBS's Joint Union/Management Task Force on Diversity and Inclusion, "an inclusive workforce is fair, equitable, supportive, welcoming and respectful. It recognizes, values and leverages differences in identities, abilities, cultures, skills, experiences and perspectives that support and reinforce Canada's evolving human rights framework."[154] Unlike measures for diversity, most notably employment rates for designated groups, inclusion is harder to quantify and address. Indeed, there are no government-wide means of measuring organizational progress on inclusion, as discussed in paragraph 70.

84. Based on the definition of an inclusive workforce, the Committee identified three important areas to review. The first is the prevalence of harassment, violence and discrimination in the security and intelligence community and organizational efforts to address those issues.[155] The second is efforts to promote members of designated groups. As this review shows, members of designated groups are consistently underrepresented in leadership positions. The third is organizational efforts to engage designated groups in policies and processes related to diversity and inclusion. Such engagement is not only important to recognize, value and leverage differences, but is also a requirement imposed on organizations by the *Employment Equity Act*. Each area is addressed in turn below.

Harassment, violence and discrimination

85. In Budget 2018, the government identified combatting violence in the workplace and ensuring that workplaces are harassment-free as goals.[156] According to the report from the Clerk's Deputy Minister Task Team on Harassment, organizations across the public service have a responsibility to provide their employees with "a safe and healthy work environment that is free from all forms of harassment and inappropriate behaviours."[157] However, perceptions of harassment, violence and discrimination are still present in most organizations of the government, including the security and intelligence community.

---

[154] TBS, *Building a Diverse and Inclusive Public Service: Final Report of the Joint Union/Management Task Force on Diversity and Inclusion*, December 2017. https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/building-diverse-inclusive-public-service-final-report-joint-union-management-task-force-diversity-inclusion.html.

[155] According to the *Act to Amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act, 2017, No.* 1, "harassment and violence means any action, conduct or comment, including of a sexual nature that can reasonably be expected to cause offence, humiliation or other physical or psychological injury or illness to an employee, including any prescribed action, conduct or comment." *Act to Amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act, 2017, No.1* , S.C. 2018, c. 22, s. 0.1.

[156] Canada, *Budget 2018*.

[157] Canada, *Safe Workspaces: Starting a Dialogue and Taking Action on Harassment in the Public Service*, Report from the Deputy Minister Task Team on Harassment, 2018, https://www.canada.ca/en/privy-council/corporate/clerk/publications/safe-workspaces.html.

86. TBS defines *harassment* as:

> improper conduct by an individual, that is directed at and offensive to another individual in the workplace, including at any event or location related to work, and that the individual knew or ought reasonably to have known would cause offence or harm. It comprises objectionable act(s), comment(s) or display(s) that demean, belittle, or cause personal humiliation or embarrassment, and any act of intimidation or threat. It also includes harassment within the meaning of the *Canadian Human Rights Act* (i.e. based on race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and pardoned conviction).[158]

87. TBS defines *discrimination* as:

> Treating someone differently or unfairly because of a personal characteristic or distinction, which, whether intentional or not, has an effect that imposes disadvantages not imposed on others, or that withholds or limits access that is given to others. There are [13] grounds of discrimination under the *Canadian Human Rights Act*: race, national or ethnic origin, colour, religion, age, sex, sexual orientation, gender identity or expression, marital status, family status, genetic characteristics, disability, and pardoned conviction or suspended record.[159]

88. Three core organizations in the security and intelligence community have faced lawsuits alleging harassment, discrimination or violence. Most prominently, the CAF and the RCMP have faced or are currently facing class-action lawsuits alleging longstanding systemic issues of harassment, violence and discrimination in the workplace, with some lawsuits leading to official apologies and settlements totalling over $1 billion.[160] CSIS also settled a multi-million dollar lawsuit in 2017 with five employees in the Toronto Region office specifically alleging Islamophobia, racism and homophobia.[161] During the same period, reviews of organizational culture for all three organizations revealed important problems.

---

[158] TBS, *Policy on Harassment Prevention and Resolution*, June 2013, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26041#appA.
[159] Canada, Public Service Employee Survey definition of discrimination, www.tbs-sct.gc.ca/pses-saff/2017-2/results-resultats/bq-pq/00/dem114-eng.aspx#s9.
[160] In 2016 and 2019, the RCMP settled two class-action lawsuits over allegations by female officers and civilian members of "harassment, discrimination and sexual abuse." In 2017, CSIS settled a lawsuit by five intelligence officers and an analyst specifically alleging Islamophobia, racism and discrimination. In 2019, DND/CAF settled a class-action lawsuit on allegations of "rampant sexual misconduct in the military." See: Kathleen Harris, "Mounties offer apology and $100M for compensation for harassment, sexual abuse against female members," *CBC*, October 6, 2016, www.cbc.ca/news/politics/rcmp-paulson-compensation-harassment-1.3793785; RCMP, "Announcement of settlement in the Tiller et al. class action lawsuit," News release, July 8, 2019, www.rcmp-grc.gc.ca/en/news/2019/announcement-settlement-the-tiller-et-al-class-action-lawsuit; and Catharine Tunney, "Ottawa sets aside $900M to settle sexual misconduct lawsuits against Canadian Armed Forces," *CBC*, July 18, 2019, www.cbc.ca/news/politics/military-sexual-misconduct-settlement-1.5216307.
[161] Michelle Shephard, "CSIS settles multimillion-dollar lawsuit with employees who claimed workplace Islamophobia, racism and homophobia," *Toronto Star*, December 14, 2017, www.thestar.com/news/canada/2017/12/14/csis-settles-multimillion-dollar-lawsuit-with-employees-who-claimed-workplace-islamophobia-racism-and-homophobia.html.

A 2015 review by former Supreme Court Justice Marie Deschamps, entitled *External Review into Sexual Misconduct and Sexual Harassment in the Canadian Armed Forces*, found "an underlying sexualized culture . . . that is hostile to women and LGBTQ members."[162] A 2017 Workplace Climate Assessment of CSIS's Toronto Region office noted problems of abuse of authority and fear of reprisal, and a lack of trust in management.[163] Finally, a 2017 review of organizational culture at the RCMP by the Civilian Review and Complaints Commission noted the long-standing issues of harassment and confirmed "problems of workplace bullying and harassment persist."[164]

89. These organizations have responded to the workplace harassment, discrimination and violence issues through a variety of programs and initiatives. CSIS implemented a Workplace Action Plan in 2017 to address organizational culture issues. The RCMP and the Minister of Public Safety and Emergency Preparedness announced the creation of an Interim Management Advisory Board in January 2019 to advise the agency on how to improve its policies and procedures on harassment in the workplace, among other things.

90. The CAF has conducted surveys to examine harassment within the armed forces. However, according to the 2012 Canadian Forces Workplace Harassment Survey, "much of the research examining harassment in the CAF was conducted in the 1990s, with minimal comprehensive research conducted since then." The 2012 survey was the last comprehensive survey on workplace harassment conducted on harassment in the regular forces and the low response rate represented "a key source of bias" in the results.[165] Similar surveys conducted on reservists, cadets and those completing Basic Military Qualifications were completed in 2015.[166] The CAF launched Operation HONOUR in June 2015 to resolve and prevent issues of sexual harassment in the armed forces.[167] The CAF has monitored force-wide perceptions on harassment regularly in the last five years as part of a much larger survey that examines a wide range of personnel issues, policies and experiences for CAF members.[168]

91. Progress on these issues has been slow. The CAF has acknowledged that eradicating harassment and violence requires a transformation of its organizational culture over the long term and has not yet

---

[162] Marie Deschamps, *External Review into Sexual Misconduct and Sexual Harassment in the Canadian Armed Forces*, External Review Authority, March 26, 2015.
[163] ADR Education Management, Workplace Climate Assessment: Toronto Region, August 2017.
[164] Civilian Review and Complaints Commission, *Report into Workplace Harassment in the RCMP*, April 2017.
[165] CAF, The 2012 Canadian Forces Workplace Harassment Survey (CFWHS): Findings from the Regular Force by Organizational Affiliation, December 2013.
[166] CAF, The Canadian Forces Workplace Harassment Survey (CFWHS): Basic Military Qualification (BMQ) administration, January 11, 2016; and The Canadian Forces Workplace Harassment Survey (CFWHS): Cadet Organizations Administration and Training Service (COATS), November 15, 2015; and The Canadian Forces Workplace Harassment Survey (CFWHS): Primary Reserve Force Administration, September 10, 2015.
[167] Canada, Operation HONOUR, www.canada.ca/en/department-national-defence/services/benefits-military/conflict-misconduct/operation-honour.html.
[168] CAF has conducted the "Your Say Survey" since 2013, but not all questions on harassment were included until 2014. CAF, Harassment and discrimination: A trend analysis of the perceptions of Canadian Armed Forces' Regular Force members (2013–2016), October 2018.

established a deadline for this initiative.[169] Several reviews of the CAF's efforts in this regard have found that the organization has made limited progress over the past four years. In 2019, Statistics Canada found that the prevalence of sexual assault in the CAF in 2018 was similar to that of 2016. The CAF's own 2019 Operation HONOUR progress report noted that the department has implemented only three of the ten recommendations from the 2015 report by Justice Deschamps.[170] A May 2019 report from the Standing Senate Committee on National Security and Defence stated that measures put in place by the CAF in the last four years to address these issues "fall short of what is required, and that further work remains to be done."[171] Similar to the CAF, the RCMP has struggled to address the pervasive issues of harassment and violence in the workplace. The Civilian Review and Complaints Commission noted in its 2017 report on harassment at the RCMP that "after each new harassment scandal has arisen, highlighting anew the RCMP's dysfunctional organizational culture, the RCMP's reaction has been merely to circle the wagons."[172] The report goes on to state "If the last ten years, over 15 reports and hundreds of recommendations for reform have produced any lessons, it is that the RCMP is not capable of making the necessary systemic changes of its own accord."[173]

92. Harassment and discrimination are also present in the other organizations under review. The following text box highlights results from the 2017 Public Service Employee Survey (PSES), an annual anonymous survey used to measure public service employees' opinions on their workplace.[174] The text box includes comparisons of the average rates of harassment and discrimination across the public service with the rates of harassment and discrimination at CBSA, CSE, DND, GAC, PCO, Public Safety Canada and the RCMP as reported in the 2017 PSES. CSIS and the CAF are not included because they do not participate in the PSES. CSIS separately administered a survey to its employees in 2015. The CAF captures its members' opinions through Canadian Forces Workplace Harassment surveys and an annual Your Say Survey.

---

[169] Brigadier General M. A. J. Carignan stated in an article for *The Maple Leaf* magazine of the Canadian Army that "although Operation HONOUR began more than three years ago, there is no completion deadline. There is clearly a lot more work to be done, and Operation HONOUR is here to stay." See: Brigadier General M. A. J. Carignan, "Brigadier-General Carignan on progress of Operation HONOUR within 2nd Canadian Division," *The Maple Leaf*, December 17, 2018.

[170] See: Statistics Canada, "Sexual Misconduct in the Canadian Armed Forces 2018", May 22, 2019, www150.statcan.gc.ca/n1/daily-quotidien/190522/dq190522a-eng.htm?CMP=mstatcan; DND/CAF, "Part 5 – Progress on the ERA Recommendations," *Canadian Armed Forces Progress Report #4 Addressing Sexual Misconduct*, February 26, 2019, www.canada.ca/en/department-national-defence/corporate/reports-publications/sexual-misbehaviour/progress-report-four/part-five.html.

[171] Senate Standing Committee on National Security and Defence, *Sexual Harassment and Violence in the Canadian Armed Forces*, 42nd Parliament, 1st Session, May 16, 2019.

[172] Civilian Review and Complaints Commission, *Report into Workplace Harassment in the RCMP*, April 2017.

[173] Civilian Review and Complaints Commission, *Report into Workplace Harassment in the RCMP*, April 2017.

[174] The results reflect the perspective of employees, not the actual number of harassment or discrimination complaints received in the past two years. The response rate for the federal public service overall was 61.3%, and information was not available on the individual response rates for each organization under review. See: Canada, 2017 Public Service Employee Annual Survey Results, www.tbs-sct.gc.ca/pses-saff/2017/results-resultats/bq-pq/index-eng.aspx.

2017 Public Service Employee Survey results for harassment and discrimination

The 2017 PSES results revealed the following:

- Of the employees in the public service who responded to the survey, 18% indicated they had been victims of harassment and 8% indicated they had been victims of discrimination in the workplace in the past two years.

Harassment

- In the public service, 19% of women employees, 28% of Aboriginal employees, 18% of employees who are members of visible minorities and 37% of employees with disabilities indicated they had been victims of harassment at work in the past two years.
- In half of the organizations under review, women experienced harassment at a higher rate than the public service average.
- In half of the organizations under review, persons with disabilities experienced harassment at a higher rate than the public service average.

Discrimination

- In the public service, 8% of women employees, 15% of Aboriginal employees, 13% of employees who are members of visible minorities and 25% of employees with disabilities indicated they had been victims of discrimination at work in the past two years.
- In a majority of the organizations under review, women experienced discrimination at a higher rate than the public service average.
- In half of the organizations under review, members of visible minorities experienced discrimination at a higher rate than the public service average.
- In a majority of the organizations under review, persons with disabilities experienced discrimination at a higher rate as compared with the public service average.

CBSA

- The rates of harassment and discrimination for all designated groups are higher at CBSA than the public service average.

Analyzing survey results and tracking complaints

93. The Deputy Minister Task Team on Harassment highlighted the importance of data analysis in identifying and addressing harassment in the workplace.[175] The report recommends that organizations "use quantitative and qualitative tools to gain a clearer line of sight to areas where harassment is more likely to occur."[176] Some of the organizations under review have sought to better understand the prevalence of harassment and discrimination and employee well-being in their organization by analyzing PSES results, conducting additional surveys and tracking harassment and violence complaints. CBSA, GAC, PCO and DND produced detailed analyses of PSES results for designated groups broken down by sources of harassment and discrimination.[177] CSE and the RCMP did not conduct an analysis of PSES results broken down by designated group. CSIS and CSE conducted internal surveys on employee well-being separate from the PSES, although CSE did not analyze the results of these surveys by designated group.[178] DND and the CAF are developing a "Defence Workplace Well-being Survey" to measure the psychological health and well-being of their workforce.[179]

94. A majority of the organizations under review track and report on the number of official harassment complaints. That said, the RCMP, DND and the CAF noted deficiencies with their tracking systems. The RCMP reported that complaints about workplace issues that do not meet the definition of harassment are still directed to the harassment process in the absence of alternative forms of formal recourse, effectively skewing the statistics.[180] DND and the CAF characterized their joint Harassment Complaint Tracking System, in place since 2012, as "highly under-utilized" by individuals responsible for inputting information about harassment complaints.[181] DND continues to use this system to track

---

[175] Canada, *Safe Workspaces: Starting a Dialogue and Taking Action on Harassment in the Public Service*, Report from the Deputy Minister Task Team on Harassment, 2018, www.canada.ca/en/privy-council/corporate/clerk/publications/safe-workspaces.html.

[176] Canada, *Safe Workspaces: Starting a Dialogue and Taking Action on Harassment in the Public Service*, Report from the Deputy Minister Task Team on Harassment, 2018, www.canada.ca/en/privy-council/corporate/clerk/publications/safe-workspaces.html.

[177] GAC, 2017 Public Service Employee Survey Results Analysis for Global Affairs Canada Canada-based Staff and Public Service respondents Aboriginal vs. Non-Aboriginal respondents, Not a person with a disability vs. Person with a disability respondents, Visible minority vs. Non-visible minority respondents, and Women vs. Men respondents, undated; CBSA, 2017 Public Service Employee Survey Results: CBSA Results, May 2018; PCO, 2017 Public Service Employee Annual Survey: Detailed Employment Equity Group Results for the Privy Council Office, undated; and DND, 2017 PSES results by EE [Employment Equity] group DND, undated.

[178] CSIS administers an internal employee survey similar to the PSES, and in 2016 it administered the Psychological Health, Safety and Wellness Survey. In 2016–2017, CSE administered its first annual Vital Signs survey, which addressed issues of organizational performance and harassment. CSIS, Psychological Health, Safety and Wellness Survey 2016, May 1, 2017; and CSE, *2016–2017 Annual Report to the Minister of Defence*, undated.

[179] DND/CAF, *The Joint Department of National Defence and Canadian Armed Forces Annual Multiculturalism Report 2017/2018*, undated.

[180] NSICOP Secretariat consultation with RCMP, Director of the Workplace Culture and Employee Engagement Unit, April 5, 2019. RCMP Regular Members certified the National Police Federation as their first-ever bargaining agent on July 12, 2019. This move may affect the organizations' grievance process going forward. CBC News, "National Police Federation wins right to represent Mounties in collective bargaining," *CBC*, July 12, 2019.

[181] DND and CAF, Written communications, May 8, 2019. The 2015 Deschamps report on sexual misconduct in the CAF stated that the "very low number of complaints that are reported each year" through the Harassment Complaint Tracking System "create a misleading picture of the problem." The Auditor General's 2018 report on sexual misconduct in CAF stated "there was

complaints, but the CAF established a separate Integrated Complaint Registration and Tracking System in 2018.[182]

95. Concerns over the accuracy of complaint tracking systems point to a larger issue of employee willingness to report harassment and discrimination. The Deputy Minister Task Team on Harassment noted "many cases of workplace harassment are never reported" due to a lack of trust or awareness of the process, or for fear of retaliation.[183] In fact, CSIS's 2015 Employee Survey found that the most frequently cited reason for not filing a formal harassment complaint was that individuals "did not believe it would make a difference."[184] That said, several of the organizations under review have made efforts to explain and build trust in the complaint process, through training and information guides.[185]

Anti-harassment policies and corrective training

96. In accordance with TBS policy, all of the organizations under review have instituted a policy on workplace harassment and violence.[186] However, a 2017 ESDC report on harassment and sexual violence in the workplace identified several problems with the existing federal legal and regulatory framework for harassment and violence in the workplace.[187] Two central findings were that the current prevention regime "does not appropriately address the range of inappropriate workplace behaviours" and that regulations in place in federally regulated workplaces "fail to outline provisions for harassment."[188] *The Act to Amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and*

---

no centralized system to track incidents of inappropriate sexual behaviour in a systematic way – the information came from many different databases and was therefore not consistent." See: Marie Deschamps, "External Review into Sexual Misconduct and Sexual Harassment in the Canadian Armed Forces," External Review Authority, March 26, 2015; and Auditor General of Canada, "Report 5 – Inappropriate Sexual Behaviour – Canadian Armed Forces," *2018 Fall Reports of the Auditor General of Canada to the Parliament of Canada*, November 2018.

[182] DND/CAF noted that DND is "currently in discussions with CAF to replace the HCTS [Harassment Complaint Tracking System] with the Integrated Complaint Registration and Tracking System." DND/CAF, Written communication to NSICOP, July 5, 2019.

[183] According to Statistics Canada's report on sexual misconduct in the CAF in 2018, 57% of victims of sexual assault in the Regular Force "said that the incidents did not come to the attention of anyone in authority," and 40% of victims in the Primary Reserves "cited a fear of negative consequences as a reason for not reporting sexual assault." See: Statistics Canada, "Sexual Misconduct in the Canadian Armed Forces 2018," May 22, 2019, www150.statcan.gc.ca/n1/daily-quotidien/190522/dq190522a-eng.htm?CMP=mstatcan; and Canada, *Safe Workspaces: Starting a Dialogue and Taking Action on Harassment in the Public Service*, Report from the Deputy Minister Task Team on Harassment, 2018, www.canada.ca/en/privy-council/corporate/clerk/publications/safe-workspaces.html.

[184] CSIS, 2015 CSIS Employee Survey, undated.

[185] DND has developed posters and encourages managers to educate employees about their rights and the complaint process. DND written communications, May 8, 2019. CSIS, in turn, has developed information guides on the harassment process, including a manager's guide on "Restoring the Workplace Following a Harassment Complaint," and a guide for employees on how to identify a possible instance of harassment. CSIS documents include "Restoring the Workplace Following a Harassment Complaint: A Manager's Guide," "Is it Harassment? A Tool Guide for Employees," "Guide on Applying the Harassment Resolution Process," and "Preventing and Resolving Harassment in the Workplace – A Guide for Managers," undated.

[186] TBS, *Policy on Harassment Prevention and Resolution*, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26041.

[187] See: Employment and Social Development Canada (ESDC), Harassment and Sexual Violence in the Workplace Public Consultations: What We Heard, November 2, 2017; and ESDC, Proposed Regulatory Framework: Harassment and Violence, Consultation Paper, Labour Program Stakeholder Consultations, August 24, 2018.

[188] ESDC, Proposed Regulatory Framework: Harassment and Violence, Consultation Paper, Labour Program Stakeholder Consultations, August 24, 2018.

Staff Relations Act and the Budget Implementation Act, 2017, No. 1, modified the existing framework for harassment and violence prevention in federally regulated workplaces.[189] The Act requires employers to take measures to prevent and protect against workplace harassment, respond to occurrences of harassment and violence, and support affected employees. Employers are also required to "investigate, record and report" all occurrences of harassment and violence.[190] As a result, the majority of organizations under review must update their harassment policies with the coming into force of this Act in the next two years.[191]

97. Organizations have instituted mandatory anti-harassment training for all employees. In most organizations, employees take the course online and are required to complete it once during their career. The exceptions are DND and the CAF, which have instituted mandatory in-person harassment prevention and bystander intervention training for all employees, including supervisors and managers.[192] The issue of discrimination receives significantly less attention, despite its prevalence across the organizations under review. CBSA is the only organization of those reviewed to require employees or managers to complete training on anti-racism and discrimination.[193]

Promotions, professional development and mentorship opportunities

98. Fair and equal access to promotional and training opportunities are key components of an inclusive workplace.[194] The Committee's review of promotion rates and professional development and mentorship opportunities revealed the following:

---

[189] The amendments to the *Canada Labour Code* do not apply to CAF. Mayra Perez-Leclerc, Legislative Summary of Bill C-65: An Act to amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act, 2017, No. 1, Publication No. 42-1-C65-E, Parliamentary Information and Research Service, February 4, 2019, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/421C65E#a3.

[190] Mayra Perez-Leclerc, Legislative Summary of Bill C-65: An Act to amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act, 2017, No. 1, Publication No. 42-1-C65-E, Parliamentary Information and Research Service, February 4, 2019, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/421C65E#a3.

[191] Mayra Perez-Leclerc, Legislative Summary of Bill C-65: An Act to amend the Canada Labour Code (harassment and violence), the Parliamentary Employment and Staff Relations Act and the Budget Implementation Act, 2017, No. 1, Publication No. 42-1-C65-E, Parliamentary Information and Research Service, February 4, 2019, https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/421C65E#a3.

[192] DND/CAF, Annex A – Required, Mandatory and Sub-delegation Training Requirements for Civilian and Military Personnel, October 11, 2018.

[193] In 2017–2018, DND/CAF offered one course on anti-discrimination but only 83 employees complete the course. The 2017 employment systems review for CSE found that "with the exception of the anti-harassment training, there is no training for HR staff, executives, managers or members of the Diversity and Employment Equity Committee with respect to systemic discrimination, how systemic discrimination operates and the requirements of the *Employment Equity Act*." See: DND/CAF, *The Joint Department of National Defence and Canadian Armed Forces Annual Multiculturalism Report 2017/2018*, undated, and Linda Buchanan, Employment Systems Review and *Employment Equity Act* Compliance Assessment: Communications Security Establishment, March 31, 2017.

[194] Quinetta M. Roberson, "Disentangling the Meanings of Diversity and Inclusion," Centre for Advanced Human Resources Studies Working Paper Series, *Cornell University*, 2004.

- *Promotion rates:* For a majority of the organizations under review, including the CAF, CSE, CBSA ITAC and the RCMP, the rates of promotion for each designated group overall were proportionate to their overall representation within the organization. Promotion rates for persons with disabilities is below the average promotion rate at DND. However, few of the organizations under review provided promotion rates broken down by occupational category, making it difficult to know whether promotions for designated groups are distributed across all occupational groups or concentrated in specific areas of the workforce.
- *Professional development training:* Few organizations provided information on targeted professional development training or on access to this type of training. Two exceptions were leadership training opportunities for women at CSIS, and GAC's participation in the Crown-Indigenous Relations and Northern Affairs Canada Aboriginal Leadership Development Training initiative.[195]
- *Mentorship*: While some organizations in the security and intelligence community have established formal mentoring programs, few of them target specific designated groups.[196] Two exceptions are CBSA's Visible Minority Advisory Committee Mentoring Program and the informal mentorship program established by the CSIS Women's Network.[197]

Employee engagement

99. The *Employment Equity Act* requires every employer to consult with its employees' representatives on two areas. The first is on the assistance that representatives could provide to the employer to facilitate the implementation of employment equity in its workplace and the communication to its employees of matters relating to employment equity. The second is on the preparation, implementation and revision of the employer's equity plan.[198] The main forum for designated group members to express concerns or provide input on diversity and inclusion issues are employee-led advisory committees. Membership on advisory committees is voluntary and should include representatives of all designated groups.

100. Every organization under review has established one or more advisory committees, but their degree of input on organizational policies differs across organizations. By way of example, the advisory committees for CBSA, CSIS, GAC and PCO provide regular input on employment policies and practices.[199] The RCMP recently consolidated all of its advisory committees and formally integrated the committee

---

[195] Professional development opportunities for women offered by CSIS include the "Taking the Stage" course offered by the Niagara Institute and a course at Carleton University entitled "Advancing Women in Leadership." See: CSIS, Justification for Sole Source Delivery – Employee Development/Talent Management/Learning and Development: Achieving Gender Equity at Senior Levels, January 16, 2017; and GAC, Diversity & Inclusion (D&I) Presentation to Executive Board, May 2018.

[196] The RCMP and CSIS have developed a mentorship program, but neither program targets designated groups specifically. RCMP, National Headquarters Mentorship Program Guidebook, May 24, 2017; and CSIS, Mentoring Program: Mentoring Activities for Developing Leadership Competencies, January 2015.

[197] CBSA, Visible Minority Advisory Committee, October 2018; and ITAC written submission to Committee, April 10, 2019.

[198] *Employment Equity Act*, S.C. 1995, c. 44, s. 15(1), https://laws-lois.justice.gc.ca/eng/acts/e-5.401/page-2.html#docCont.

[199] Judy Laws, "Targeted Employment Systems Review for Global Affairs Canada," *Graybridge Malkam*, June 19, 2017; CSIS, CSIS Advisory Committee on Diversity Terms of Reference, August 31, 2012; CBSA, National Employment Equity and Diversity Advisory Committee, December 2010; PCO, Invitation to join the Employment Equity and Diversity Advisory Committee, December 2017.

into the employment equity planning process.[200] In contrast, CSE's 2017 employment systems reviews noted that its advisory committee's engagement on these issues was limited.[201] For its part, the CAF's 2013 employment systems review found that few military members were aware of the existence or function of its advisory committees.[202]

[200] RCMP, Refreshing the Employment Equity Planning Process, May 2018; and NSICOP Secretariat consultation with the RCMP, Director of the Workplace Culture and Employee Engagement Unit, April 5, 2019.

[201] CSE's employment systems review found that the Diversity and Employment Equity Committee does not currently review proposed human resources policies prior to their implementation. See: Linda Buchanan, Employment Systems Review and *Employment Equity Act* Compliance Assessment: Communications Security Establishment, March 31, 2017.

[202] Alla Skomorovsky and Sylvie Lalonde-Gaudreault, *Canadian Forces Employment Systems Review: Qualitative Component*, Defence Research and Development Canada, Director General Military Personnel Research and Analysis, September 2013.

Members of Visible Minorities in the Security and Intelligence Community

According to the 2016 census, members of visible minorities represent 22.3% of the population with South Asian, Chinese and Black Canadians forming the three largest minority communities. Demographic projections suggest that by 2036 members of visible minorities could represent between 31.2% and 35.9% of the total population.[203]

Members of visible minorities are underrepresented in a majority of the organizations under review, particularly at executive levels. This gap in representation will likely increase in the coming years as new WFA and LMA estimates reflect changes in the number of members of visible minorities in Canada. Data collection on this group is also incomplete given the absence of data disaggregated by sex, which obscures the representation of visible minority women in organizations.[204]

At the same time, the representation and recruitment of members of visible minorities in several organizations has stagnated or decreased in recent years. At CSE, there is a trend toward increasing underrepresentation of members of visible minorities.[205] A staffing analysis conducted by PCO revealed a decrease of 15% in all staffing actions for this group since 2014–2015.[206] At Public Safety Canada, the representation of members of visible minorities has not increased since 2012.[207] In 2018, the Canadian Human Rights Commission stated that the CAF's progress in increasing visible minority representation "will not be sufficient to keep pace with the growing number of Canadian citizens who are . . . visible minorities."[208]

Recent news reports and documents provided to the Committee also suggest that members of visible minorities continue to face attitudinal barriers. The CAF, CSIS and the RCMP have faced allegations of racism in recent years.[209] More subtle attitudinal barriers were also identified at CBSA, DND and GAC, including that members of visible minorities feel unrepresented and unheard at senior levels of the organization, and, as noted in DND's employment systems review, feel unable to "express themselves ethnically and culturally at work."[210]

---

[203] Canada, *Annual Report on the Operation of the* Canadian Multiculturalism Act *2016–2017*, https://www.canada.ca/en/canadian-heritage/corporate/publications/plans-reports/annual-report-canadian-multiculturalism-act-2016-2017.html.

[204] Judy Laws, "Targeted Employment Systems Review for Global Affairs Canada," *Graybridge Malkam*, June 19, 2017; NSICOP Secretariat consultation with representatives of the Federal Black Employee Caucus, April 16, 2019.

[205] Linda Buchanan, Employment Systems Review and *Employment Equity Act* Compliance Assessment: Communications Security Establishment, March 31, 2017.

[206] PCO, Staffing Action Employment Equity Results at PCO, February 2018.

[207] Linda Buchanan, "Final Report: Employment Systems Review, Public Safety Canada," *Mobile Resources*, March 28, 2018.

[208] Canadian Human Rights Commission, *Employment Equity Interim Audit Report: Canadian Armed Forces*, August 15, 2018.

[209] "Black RCMP officers say they endured racism 'on a regular basis'," *CBC*, March 11, 2019, www.cbc.ca/news/politics/rcmp-anti-black-racism-1.5048850; Michelle Shephard, "CSIS 'a workplace rife with discrimination,' say employees in $35-million lawsuit alleging Islamophobia, racism and homophobia," *Toronto Star*, November 7, 2017, www.thestar.com/news/canada/2017/11/07/csis-a-workplace-rife-with-discrimination-say-employees-in-35-million-lawsuit-alleging-islamophobia-racism-and-homophobia.html; Dennis Ward, "Racism and discrimination 'rampant' throughout ranks and elements of Canadian Armed Forces says report," *APTN News*, January 19, 2017, https://aptnnews.ca/2017/01/19/racism-and-discrimination-rampant-throughout-ranks-and-elements-of-canadian-armed-forces-says-report/; and Chloé Fedio, "Ex-military members claim systemic racism in lawsuit," *CBC*, December 22, 2016, www.cbc.ca/news/canada/ottawa/canadian-military-systemic-racism-class-action-suit-1.3909258.

[210] See: Sylvie C. Lalonde, *The 2009-2010 Department of National Defence Employment Systems Review: Workforce Component*, Civilian Personnel Research and Analysis, Personnel and Family Support Research, DND/CAF, July 2011; GAC, Notes from the meetings between Leslie Norton and Global Affairs Canada Employment Equity Network Representatives, August 15–18 and 28–29, and September 7 and 22, 2017; CBSA, Learning Evaluation Data Summary Report Diversity and Race Relations H1000-P, July 18, 2018; and NSICOP Secretariat consultation with representatives of the Federal Black Employee Caucus, April 16, 2019.

The Committee's assessment of organizational efforts to foster inclusion

101. The Committee believes that an essential feature of an inclusive workplace is the absence of harassment, violence and discrimination. The importance of these issues cannot be overemphasized. The slow pace of progress in eradicating harassment, violence and discrimination at the CAF and the RCMP is of serious concern. In addition, while organizations across the community have implemented anti-harassment policies, training and awareness campaigns, many still have a limited understanding of the prevalence and sources of harassment in their workforce. The issue of discrimination, in turn, has received considerably less attention across all the organizations. In addition, employee engagement on diversity and inclusion is inconsistent across organizations under review, potentially undermining broader efforts to foster inclusion throughout the organizations. Finally, in the Committee's view, issues of underrepresentation and allegations of discrimination against members of visible minorities in the security and intelligence community require further study. The operational imperative for greater diversity combined with accelerating demographic change suggest that issues affecting members of this designated group require additional attention.

Conclusion

102. Building diverse and inclusive workforces is essential to the effectiveness of the security and intelligence community. It is imperative that organizations charged with the responsibility to defend Canada and protect Canadians leverage the skills, talent and perspectives of individuals of different genders, abilities, and racial, ethnic, cultural and religious backgrounds. That belief is well-founded in academic and professional studies and the approaches of Canada's closest allies. Most importantly, it is also shared by the senior leadership of the security and intelligence organizations themselves. Unfortunately, there is still much work to be done. Levels of underrepresentation for designated groups and rates of harassment and discrimination remain unacceptably high. The corrosive allegations of harassment, violence and discrimination at the CAF and the RCMP, two core members of the security and intelligence community, remain fresh in the public's memory. Addressing these issues will require sustained leadership and a commitment from each organization to create workforces that fully reflect Canada's diversity. Given the importance of the issues involved, the Committee believes that the security and intelligence community can and should be a leader within the wider public service.

Going forward

103. The Committee believes that it will be important to track the community's progress in increasing the representation of designated groups in all occupational groups and strengthening inclusion in the coming years. Indeed, the operational imperative for diversity across the security and intelligence community combined with Canada's evolving demographics suggests that continued improvement in these areas is critical to the success of these organizations. Moreover, given the long-term nature of organizations' representation goals and inclusion initiatives, a review of their implementation may serve as an indicator of the pace of progress on diversity and inclusion across the community.

Findings

104. The Committee makes the following findings:

F1. In successive ministerial mandate letters and in its call to create a Security and Intelligence Diversity and Inclusion Tiger Team, the government identified the promotion and enhancement of diversity and inclusion as a priority in the security and intelligence community. This community approach has significant merit, but its implementation has fallen short. (Paragraphs 22, 68 and 69)

F2. Organizations in the security and intelligence community have put in place measures and programs to support employment equity, diversity and inclusion. However, the degree to which those organizations are diverse and inclusive differs significantly. (Paragraphs 36–50)

F3. In the past three years, the CAF and the RCMP settled lawsuits variously alleging widespread harassment, violence and discrimination. Progress on resolving and eradicating these underlying problems has been slow. CSIS also settled a lawsuit in 2017 specifically alleging Islamophobia, racism and homophobia in its Toronto Region office, and responded with an organization-wide Workplace Action Plan that same year. (Paragraphs 88–91)

F4. All of the organizations in the security and intelligence community have developed policies, training and awareness campaigns to combat and resolve harassment and violence in the workplace. However, some challenges exist with regard to survey analysis and tracking. This includes tracking harassment complaints, which can limit an organization's awareness of its prevalence. The issue of discrimination receives significantly less attention than harassment throughout the community. (Paragraphs 93–97)

F5. The representation of designated groups is lower than the public service average in a majority of the organizations under review. In a majority of the organizations under review, persons with disabilities are underrepresented overall and women are underrepresented at executive levels. Members of visible minorities are underrepresented both overall and at executive levels, and recruitment of members of visible minorities has stalled or decreased in several of the organizations under review over the past three years. There is currently not enough information available to assess the representation of Aboriginal peoples at executive levels across organizations under review. (Paragraphs 52–54)

F6. Inconsistencies in planning, monitoring and review undermine efforts to assess progress on diversity across the security and intelligence community. (Paragraphs 25–31)

F7. Accountability for diversity and inclusion across the security and intelligence community is insufficient. Organizations have not developed performance measurement frameworks, nor have they established measurable performance objectives for diversity and inclusion for executives or managers. Responsibility for advancing diversity and inclusion is not shared throughout most organizations, but is most often considered the sole responsibility of human resources divisions. Weaknesses in the areas of accountability and responsibility undermine organizational efforts to advance organization-wide objectives. (Paragraphs 66–71)

Recommendations

105. The Committee makes the following recommendations:

R1.	The Committee conduct a retrospective review in three to five years to assess the security and intelligence community's progress in achieving and implementing its diversity goals and inclusion initiatives, and to examine more closely the question of inclusion, including issues of harassment, violence and discrimination, through closer engagement with employees.
R2.	The security and intelligence community adopt a consistent and transparent approach to planning and monitoring of employment equity and diversity goals, and conduct regular reviews of their employment policies and practices (that is, employment systems reviews) to identify possible employment barriers for women, Aboriginal peoples, members of visible minorities and persons with disabilities.
R3.	The security and intelligence community improve the robustness of its data collection and analysis, including GBA+ assessments of internal staffing and promotion policies and clustering analyses of the workforce. In this light, the Committee also highlights the future obligation for organizations to investigate, record and report on all occurrences of harassment and violence in the workplace.
R4.	The security and intelligence community develop a common performance measurement framework, and strengthen accountability for diversity and inclusion through meaningful and measurable performance indicators for executives and managers across all organizations.

Chapter 2: The Government Response to Foreign Interference

Introduction

106. For almost 20 years, the government has rightly focused on terrorism as the greatest threat to public safety. While that threat persists, the Director of the Canadian Security Intelligence Service (CSIS) recently identified foreign interference and espionage as the greatest threat to Canadian prosperity and national interests. He stated that "activities by hostile states can have a corrosive effect on our democratic system and institutions."[1]

107. Foreign states attempt to influence Canada, its decision-making and its people through activities ranging from overt and often friendly forms of normal diplomatic conduct on the one hand to covert and hostile actions on the other. The CSIS Act makes the distinction between acceptable and unacceptable behaviour of foreign states by defining foreign influence as activities that are "detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person." The term "foreign influence" is also used in other legislation, including the *Security of Information Act*. That said, the term "foreign interference" has become common in Canada and among its allies to better distinguish between acceptable diplomatic practices and hostile or illegal practices. This report uses "foreign interference," but emphasizes that its definition is identical to that of "foreign influence" in the CSIS Act.

108. Foreign interference activities can include using deceptive means to "cultivate relationships with elected officials and others perceived to possess influence in the political process; seek to influence the reporting of Canadian media outlets; seek, in some cases, to affect the outcome of elections; and coerce or induce diaspora communities to advance foreign interests in Canada."[2] There are multiple consequences of foreign interference, including undermining:

- democratic rights and fundamental freedoms of Canadians;
- the fairness and openness of Canada's public institutions;
- the ability of Canadians to make informed decisions and participate in civic discourse;
- the integrity and credibility of Canada's parliamentary process; and
- public trust in the policy decisions made by the government of the day.[3]

109. While the use of cyber tools as a form of foreign interference has received significant media attention, [*** person-to-person foreign interference remains a common practice ***],[4] which the Committee characterizes as traditional foreign interference. As a multicultural society with an open and

---

[1] Canadian Security Intelligence Service (CSIS), Director, Speech to the Economic Club of Canada, December 4, 2018, www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.

[2] CSIS, Meeting with Acting Minister of Democratic Institutions: Director's Speaking Notes, March 23, 2018.

[3] Privy Council Office (PCO), Hostile State Activity: Identifying Canada's Strategic Interests, September 2018.

[4] CSIS, *** undated.

democratic system, Canada is vulnerable to foreign actors seeking to interfere with its political and economic processes. As will be demonstrated throughout the report, hostile states exploit or threaten rights and freedoms that are protected by the *Canadian Charter of Rights and Freedoms*, including freedom of conscience and religion, freedom of thought and expression, freedom of the press, freedom of association, democratic rights, mobility rights, security of the person, and the rule of law. In short, foreign interference threatens the fundamental values of our country. In many cases, foreign states target Canadian communities, particularly diaspora or ethnocultural communities, to influence Canada's position domestically and internationally on political, economic or social issues. The report will highlight that some foreign states "threaten to compromise Canadian sovereignty when [their] interests are judged to differ from Canada's."[5]

110. Canada's allies have identified foreign interference as a significant threat and have initiated various countermeasures. Notably, foreign interference in Australia, New Zealand and the United States has been the subject of significant public discussion and academic research. In contrast, foreign interference in Canada has received minimal media and academic coverage, and is not part of wider public discourse.

111. This has resulted in the assumption that foreign interference is not a significant problem in Canada. For example, in examining foreign interference from the People's Republic of China, a 2018 report by the Hoover Institution in the United States stated that "Canadian experiences with Chinese interference are less intense than those documented in Australia and New Zealand." It also noted that "the view in Ottawa is that China is definitely trying to influence Canadian opinion and opinion-makers but is not making much headway at present."[6]

112. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a CSIS assessment. ***][7] ***[8]

113. Foreign interference activities predominantly threaten the fundamental building blocks of Canada's democracy. These include "an independent media that follows journalistic ethics and editorial accountability; an empowered and protected civil society; and civic education to build a resilient citizenry."[9] These fundamental principles and institutions support effective, accountable and transparent government but also represent vulnerabilities through which foreign states seek to covertly and inappropriately interfere with Canada.

---

[5] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018.
[6] Hoover Institution, *Chinese Influence and American Interests: Report of the Working Group on Chinese Influence Activities in the United States*, 2018.
[7] CSIS, *** Briefing note to Director, August 2018.
[8] CSIS, Director, *** 2018.
[9] Global Affairs Canada (GAC), Reinforcing Democracy – Addressing Foreign Interference Issue Note, February 28, 2018.

Overview of the review

114. On November 6, 2018, the Committee decided to undertake a review of foreign interference in Canada. The Committee was conscious that given the highly sensitive nature of the material, much of the public version will be redacted. On December 6, 2018, the Chair of the Committee provided notification letters to the Prime Minister and the ministers of Foreign Affairs, National Defence, and Public Safety and Emergency Preparedness. The review included the following organizations:

- Canada Border Services Agency (CBSA);
- Canadian Security Intelligence Service (CSIS);
- Communications Security Establishment (CSE);
- Global Affairs Canada (GAC);
- Privy Council Office (PCO);
- Public Safety Canada (PS); and
- the Royal Canadian Mounted Police (RCMP).

115. The Committee informed the ministers involved that the review would narrow in focus as it progressed, but would begin with an examination of:

- the extent and nature of the threat and the actors involved;
- the mandates and roles of the relevant organizations;
- cooperation and de-confliction with allies and between departments and agencies on investigations and operations, including information sharing among federal organizations, other levels of government or non-governmental organizations;
- resourcing and prioritization of this issue within relevant departments and agencies;
- strategies for and approaches to protecting Canada's fundamental democratic institutions and structures;
- legislative frameworks for investigating, prohibiting, preventing or countering foreign interference and influence activities; and
- the implementation of and support to an intelligence priority.

116. To focus its efforts, the Committee excluded a number of issues from the scope of its review. It did not examine specific interference activities directed at the 2019 federal election given the government's recent and ongoing efforts in this area. Similarly, it did not examine cyber threats: the government has recently implemented a range of measures to counter cyber threats and the Committee decided the timing of such a review would potentially undermine their implementation. Lastly, the Committee excluded elements of the *Investment Canada Act* process, as this issue alone could form the basis of a review. Under this Act, the government may review the national security implications of foreign acquisitions of Canadian businesses, which may have implications related to foreign

interference.[10] The Committee's approach should not be viewed as discounting the range of threats posed by foreign states to Canada and its interests (e.g., espionage, hostile economic activity); rather, the Committee elected to focus the scope of its inquiry on traditional foreign interference.

117. The Committee principally examined materials produced between January 1, 2015, and August 31, 2018. It also received relevant material outside of this period. The Committee believes that this timeframe provided an appropriate basis for it to sufficiently examine the current threat environment and the government's response.

118. The Committee's review proceeded in two stages. The first was an examination of government material that described the nature and scope of the threat posed to Canada by foreign interference activities and the main states involved. The Committee supplemented this material with academic and public sources of information, as well as discussions with subject matter experts outside of government. The second stage was to assess the government's response to the threat. The Committee requested additional material from government departments and held hearings with officials between March and May, 2019. All together, government organizations provided the Committee with over 620 documents, representing over 4,300 pages of material, and 17 officials appeared before the Committee.

119. This chapter is divided into two parts. The first explains the breadth and scope of the threat of foreign interference by outlining the primary threat actors, and by examining the threat those actors pose to Canada's fundamental institutions and ethnocultural communities. The second describes government efforts to respond to the threat. Each section contains the Committee's assessment. The chapter concludes with the Committee's findings and recommendations.

[10] Innovation, Science and Economic Development Canada, "Guidelines on the National Security Review of Investments," Government of Canada, December 19, 2016, www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html.

Part I: The threat from foreign interference

States that engage in foreign interference

120. States engage in foreign interference activities to support their national interests. These interests include regime protection and domestic legitimacy; strategic advantages and spheres of influence (such as their economic, political or security agendas); projection of power and deterrence; and reputation.[11] *** perpetrators of foreign interference in Canada are the People's Republic of China (PRC) and the Russian Federation. Other states active in this area include ***[12]

121. PCO and CSIS assess that Canada is a target due to its global standing; robust and diverse economy; large ethnocultural communities; membership in key multilateral organizations such as the Five Eyes,[13] G7 and NATO; and close relationship with the United States.[14]

122. The activities explored in this chapter are illustrative and represent only a portion of hostile state activities that seek to penetrate and manipulate Canada's institutions, economy, polity and society. They should be understood as components of broader strategies directed at Canada by foreign states.

The People's Republic of China

123. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a CSIS assessment. ***][15] ***[16]

124. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes the objectives and tools of China's foreign interference. ***][17] ***[18]

- ***[19]
- ***[20]

---

[11] PCO – Intelligence Assessment Secretariat, *** Interfering with Democracy, May 28, 2018; and CSIS, Meeting with Acting Minister of Democratic Institutions: Director's Speaking Notes, March 23, 2018.

[12] ***

[13] The Five Eyes are Canada, the United States, the United Kingdom, Australia and New Zealand.

[14] PCO – Intelligence Assessment Secretariat, *** Interfering with Democracy, May 28, 2018; and CSIS, *** 2017.

[15] CSIS, *** 2017.

[16] CSIS, *** Memorandum to the Director and Deputy Director of Operations, 2017.

[17] CSIS, *** 2017.

[18] PCO – Intelligence Assessment Secretariat, *** Interfering with Democracy, May 28, 2018; and CSIS, *** 2018.

[19] The United Work Front Department of the Chinese Communist Party (CCP) is "an integral part of the Party structure, down to sometimes the lowest levels and coordinated at the very top by a United Front Leading Small Group initiated by Xi Jinping. The Department works to reach out, represent, and guide key individuals and groups within both the PRC and greater China, including Chinese diasporas. The goals include to have all such groups accept CCP rule, endorse its legitimacy, and help achieve key Party aims." Mercy A. Kuo, "China's United Front Work: Propaganda as Policy," *The Diplomat*, February 14, 2018, https://thediplomat.com/2018/02/chinas-united-front-work-propaganda-as-policy/.

[20] CSIS, Director, *** 2018; and J. Michael Cole, "The Hard Edge of Soft Power: Understanding China's Influence Operations Abroad," *Macdonald-Laurier Institute*, October 2018.

125. [*** Two sentences were revised to remove injurious or privileged information. The sentences describe tools of Chinese foreign interference. ***][21] The PRC utilizes its growing economic wealth to mobilize interference operations: "with deep coffers and the help of Western enablers, the Chinese Communist Party uses money, rather than Communist ideology, as a powerful source of influence, creating parasitic relationships of long-term dependence."[22]

126. The PRC's legislative framework directs all Chinese entities and individuals to contribute to state security. CSIS assessed that "it is likely that citizens can be compelled to assist PRC state actors in interference efforts if and when those efforts fall under the broader definition of 'national intelligence work' and 'national intelligence efforts' as noted in the Law."[23] Passed in June 2017, its National Intelligence Law:

> compels Chinese entities, including state and private sector companies, as well as Chinese citizens (regardless of whether or not they are also citizens of other countries) to cooperate with the PRC's Intelligence Services (PRCIS) and government writ-large on national security issues. . . . The [National Intelligence Law] also applies to Chinese entities and individuals operating outside China. . . . the [National Intelligence Law] creates an overt and legally enforceable framework for cooperation between the PRCIS and Chinese entities/individuals.[24]

127. This all-encompassing strategy is rooted in China's fundamental approach to statecraft and international relations. As Australian journalist and China expert John Garnaut noted in a speech to an internal Australian government seminar in 2017: "In classical Chinese statecraft there are two tools for gaining and maintaining control over 'the mountains and the rivers': The first is *wu* (weapons, violence) and the second is *wen* (language, culture). Chinese leaders have always believed that power derives from controlling both the physical battlefield and the cultural domain. You can't sustain physical power without discursive power. *Wu* and *wen* go hand in hand."[25]

128. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a briefing to the Minister of Public Safety and Emergency Preparedness. ***][26]

---

[21] CSIS, *** 2017.
[22] Jonas Parello-Plesnar and Belinda Li, "The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond," *Hudson Institute*, June 2018, https://s3.amazonaws.com/media.hudson.org/files/publications/JONASFINAL.pdf.
[23] CSIS, NSICOP Review of Foreign Interference in Canada: Draft #2 - CSIS Comments, August 9, 2019.
[24] CSIS, *** 2018.
[25] John Garnaut, "Engineers of the Soul: Ideology in Xi Jinping's China," Speech for an Australian internal government Asian strategic and economic seminar series, August 2017, https://nb.sinocism.com.
[26] CSIS, *** 2018.

The Russian Federation

129. The Russian Federation engages in foreign interference activities across Canada's political system with the objective of influencing government decision-making and swaying public opinion. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes the objectives of Russian foreign interference activities. ***][27]

130. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes tools of Russian foreign interference. ***][28] Some of Russia's *** intelligence officers under diplomatic cover have engaged in threat-related activities.[29]

131. The nature and extent of Russia's foreign interference threat is significant as these activities form a key component of the broader national security threat posed by Russia. ***[30]

Other states engaged in foreign interference

132. [*** Paragraphs 132, 133, 134 and 135 were revised to remove injurious or privileged information. Those paragraphs describe the activities of other countries which engage in foreign interference in Canada. ***][31]

133. ***[32] ***[33]

134. ***[34] ***[35]

135. ***[36] ***

---

[27] PCO – Intelligence Assessment Secretariat, *** Interfering with Democracy, May 28, 2018.
[28] Communications Security Establishment (CSE), *** March 2, 2018.
[29] Statement by the Honourable Chrystia Freeland, Canada expels Russian diplomats in solidarity with United Kingdom, March 26, 2018. ***
[30] CSIS, Minister of Foreign Affairs Brief *** undated.
[31] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018; and CSIS, *** 2016.
[32] CSIS, ***, 2016.
[33] CSIS, *** 2016; CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, 2018; and ***
[34] CSIS, Foreign Influence Activities in Canada, NSIA presentation, March 10, 2016.
[35] CSIS, Foreign Influence in Democratic Institutions Talking points for Director, June 20, 2018.
[36] CSIS, Foreign Influence Activities in Canada, May 16, 2017.

Fundamental institutions and ethnocultural communities

136. States that conduct foreign interference activities pose a threat to Canada and its fundamental institutions. The targeting and manipulation of ethnocultural communities is the primary means through which these states control messages and seek to influence decision-making at all levels of government. Some individuals willingly act as agents of a foreign power for a variety of reasons including patriotism or the expectation of reciprocal favours. These states also co-opt individuals inside and outside of ethnocultural communities through flattery, bribery, threats and manipulation. The issue of co-opted individuals will be examined within the section on interference in governance and decision-making.

Communities

137. Canada is a multicultural society, home to large ethnocultural communities. For example, there are approximately 1.8 million Canadians of Chinese background and 1.2 million Canadians of Indian background in Canada,[37] 1 in 5 Canadians were born abroad, and over 22 percent of Canadians identify their mother tongue as a language other than English, French or Indigenous languages.[38] Some of these ethnocultural communities are vulnerable to foreign interference either as targets or as a means of undermining Canadian values and freedoms, and threatening the personal liberties of Canadians and landed immigrants.

138. A great deal of foreign interference has the goal of creating a single narrative or consistent message that helps to ensure the survival and prosperity of the foreign state. As CSIS notes, ***[39] However, ethnocultural communities are not homogeneous and individuals or groups may not want to get involved or do not support the foreign state's goals. Therefore, foreign states utilize a range of tactics to enforce a single narrative. Those tactics *** include:

- threats;
- harassment;
- detention of family members abroad; and
- refusal to issue travel documents or visas.[40]

139. Many ethnocultural community members are also monitored for what the foreign state considers to be dissident views or activities. For example, [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes the foreign interference activities of a specific country in Canada and their implications for a specific ethnocultural group. ***][41]

---

[37] Lee Berthiaume, "Top federal officials warned China, India could use communities in Canada to advance agendas," The Globe and Mail, July 12, 2019, www.theglobeandmail.com/canada/article-top-officials-warned-china-india-could-use-communities-in-canada-to/.

[38] Statistics Canada, 2016 Census, February 8, 2017.

[39] CSIS, Foreign Influence Activities in Canada, Presentation to the National Security and Intelligence Advisor (NSIA), July 2018.

[40] CSIS, Meeting with Acting Minister of Democratic Institutions: Director's Speaking Notes, March 23, 2018.

[41] CSIS, *** activities in Canada *** 2018.

140. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes the foreign interference activities of a specific country in Canada and their implications for a specific ethnocultural group. ***]

***[42]

141. [*** Paragraphs 141 and 142 were revised to remove injurious or privileged information. These paragraphs describe the foreign interference activities of a specific country in Canada and their implications for a specific ethnocultural group. ***]

***[43]

142. ***

- ***
- ***
- ***
- ***
- ***
- ***
- ***
- ***[44]

***[45]

143. GAC has noted [*** that a specific state ***] is increasingly monitoring and harassing human rights defenders in Canada and interfering with freedom of assembly and media. These activities have "a chilling effect on human rights activism and freedom of expression." ***[46]

144. Similarly, the PRC is conducting covert repatriation activities targeting apparent economic fugitives and corrupt officials under its global campaign entitled Fox Hunt. The repatriation activities include clandestine and coercive measures that target and threaten individuals across the globe, including those residing in Canada.[47] This issue is considered in detail in Part II of this chapter.

---

[42] CSIS, *** 2016.
[43] CSIS, Annual Report to the Minister of Public Safety and Emergency Preparedness *2015–16*, undated.
[44] This list is *** not exhaustive and can be found in the following CSIS Intelligence Assessment (IA): *** 2015.
[45] CSIS, Foreign Influence Activities in Canada, Presentation to the NSIA, July 2018.
[46] GAC, *** January 28, 2018.
[47] Nathan Vanderklippe, "China's Fox Hunt in Canada strains trust that an extradition treaty is possible," The Globe and Mail, May 16, 2018, www.theglobeandmail.com/news/world/chinas-fox-hunt-in-canada-strains-trust-that-an-extradition-treaty-is-possible/article32042306/; and Mark Mazzetti and Dan Levine, "Obama administration warns Beijing about covert agents operating in U.S.," August 16, 2015, www.nytimes.com/2015/08/17/us/politics/obama-administration-warns-beijing-about-agents-operating-in-us.html.

Governance and decision-making

145. Canada's system of government allows Canadians to elect their representatives and for all members of Canadian society to engage in free and open debate about the direction of the country. However, this system and the sovereignty of Canadian decision-making is under direct threat from interference activities of foreign states and their proxies.

146. The threat faced by Canada's governance and decision-making institutions is not only a federal problem. Elected and public officials across all orders of government are targeted: members of the executive branch, members of Parliament, senators, members of provincial legislative assemblies, municipal officials and representatives of Indigenous governments. This targeting occurs regardless of an official's status in government or opposition. Beyond elected officials, individuals who may influence government decision-making are also targeted. While the majority of elected and appointed officials conduct their business with genuine integrity, some are wittingly or unwittingly subject to foreign interference activities, jeopardizing the integrity of Canada's system of government. Foreign interference activities are targeted at three key areas: the electoral process at all stages; elected officials and their staff; and sub-national areas of government.[48]

Targeting the electoral process at all stages

147. Foreign interference operations target the electoral process at all stages. [*** Paragraphs 147 and 148 were revised to remove injurious or privileged information. These paragraphs describe how states interfere in various aspects of Canada's electoral process. ***]

148. ***

149. The following examples illustrate the threats described above.

- ***[49]
- ***[50]
- ***[51]
- ***[52]

150. In each of these examples, the activities of the foreign state were clandestine or deceptive and clearly detrimental to the integrity of the democratic process.

---

[48] Sub-national areas of government refers to all domestic orders of government below the federal level.
[49] CSIS, *** 2015.
[50] CSIS, Foreign Influence Activities in Canada, March 10, 2016.
[51] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018.
[52] CSIS, *** 2015.

Targeting elected officials and their staff

151. Once holding public office, elected and appointed officials, their staff, and employees of the legislative assemblies can also be targeted by foreign states. At the federal level, this includes all three major political parties.

152. Foreign states will seek to influence deliberations and decision-making, and to curb initiatives deemed contrary to their interests. They will seek leverage over officials that can be used to apply pressure to enhance their interests. In other instances, foreign states will mobilize third parties, proxies and lobby groups to carry out interference activities, and in some cases the target is unaware of the nature of the activity directed at them. In other cases, foreign states may seek to interfere with policy actions by attempting to discredit or attack senior public officials.

153. Examples that illustrate foreign interference activities directed at elected officials and their staff include the following:

- ***[53]
- ***[54]
- ***[55]
- ***[56]
- ***[57]

Targeting sub-national orders of government

154. Provincial, municipal and Indigenous governments wield important power in areas that are of interest to states engaged in foreign interference activities. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a CSIS assessment. ***] [58]

155. Many of the same tactics used to target elected officials at the federal level are replicated with provincial, municipal and Indigenous officials. Illustrative examples from the last decade include the following:

- ***[59] ***[60]

---

[53] CSIS, *** January 13, 2015.
[54] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018.
[55] CSIS, *** 2015.
[56] CSIS, Foreign Influence Activities in Canada, May 17, 2016.
[57] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018; and CSIS, *** 2017.
[58] CSIS, *** 2016.
[59] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018.
[60] CSIS, Foreign Influenced Activities in Canada: Critical Threats to Canadian Democracy: Speaking Notes, July 19, 2018; and CSIS, *** 2015.

- ***[61] ***[62]
- ***[63]
- ***[64]
- ***[65]

[61] CSIS, Foreign Influence Activities in Canada, May 17, 2016.
[62] CSIS, Foreign Influence Activities in Canada, May 17, 2016.
[63] CSIS, *** 2015.
[64] CSIS, *** 2016.
[65] CSIS, Foreign Influence Activities in Canada, May 17, 2016.

Media

156. A free and independent press is the fourth estate of democratic societies. Ethical journalism rooted in accurate, fair, independent and transparent reporting helps to develop a well-informed citizenry and hold decision-makers accountable, while supporting knowledge, debate and transparency. However, foreign states may use mass media to play a role in "amplifying targeted messages, propagating disinformation, and discrediting credible news and journalists."[66]

157. Foreign interference in the media can take a variety of forms, from distorting messages and encouraging self-censorship to hostile takeovers and foreign control of media outlets. Foreign states use ethnic and mainstream media to spread messages and forward their own agendas. *** The PRC and the Russian Federation both manipulate mainstream and ethnic media.[67]

Mainstream Canadian media

158. Traditionally, the PRC took a defensive approach to the media, through domestic censorship and by expelling critical foreign journalists. More recently, the PRC has added a more assertive approach by "trying to reshape the global information environment with massive infusions of money – funding paid-for advertorials, sponsored journalistic coverage and heavily massaged positive messages from boosters. While within China the press is increasingly tightly controlled, abroad Beijing has sought to exploit the vulnerabilities of the free press to its advantage."[68]

159. The PRC uses a strategy referred to as "borrowing a boat to go out into the ocean." This strategy involves using mainstream international media to push the messages of the PRC. This often takes the form of strategic partnerships with media to provide free PRC-approved messages for China-related news, similar to a wire service.[69] Sometimes, the content is supplemental and paid for through advertisement. For example, the *China Daily* paid for multi-page supplements in large newspapers including the *New York Times*, the *Wall Street Journal*, the *Washington Post* and the UK *Telegraph*. These inserts, called "China Watch," look like part of the newspaper, but are propaganda for which the *Telegraph* alone reportedly receives £750,000 (approximately C$1.3 million) annually.[70]

---

[66] GAC, Reinforcing Democracy – Addressing Foreign Interference Issue Note, February 28, 2018.
[67] ***
[68] Louisa Lim and Julia Bergin, "Inside China's Audacious Global Propaganda Campaign," *The Guardian*, December 7, 2018, www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping.
[69] Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities Under Xi Jinping," Paper for The Corrosion of Democracy Under China's Global Influence Conference, Supported by the Taiwan Foundation for Democracy, Arlington, Virginia, USA, September 16–17, 2017, https://wilsoncenter.org/sites/default/files/for_website_magicweaponanne-mariesbradyseptember2017.pdf.
[70] Louisa Lim and Julia Bergin, "Inside China's Audacious Global Propaganda Campaign," *The Guardian*, December 7, 2018, www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping.

160. [*** Paragraphs 160, 161 and 162 were revised to remove injurious or privileged information. These paragraphs describe how certain countries manipulate and control mainstream and ethnic media. ***][71] ***[72]

161. ***

- ***
- ***
- ***
- ***[73]

162. ***[74]

Canadian foreign-language media

163. Currently, there are approximately 650 publications and 120 radio and television programs in Canada that are in languages other than French and English.[75] Some of these are heavily influenced and manipulated, either wittingly or unwittingly, by foreign states.

164. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes a CSIS assessment of the objectives of a country which conducts foreign interference activities in Canada to control media. ***][76] ***[77]

165. The PRC has several state-owned media outlets that operate in Canada including Xinhua News, People's Daily and the China News Service. ***[78] The PRC is seeking to "harmonize" international Chinese-language media with its own by attempting to merge the editorial boards of those outlets with PRC media.[79] This would result in the PRC controlling the message in Chinese-language media, thereby undermining the free and independent media in Canada.

166. [*** Paragraphs 166, 167 and 168 were revised to remove injurious or privileged information. These paragraphs describe why and how countries that conduct foreign interference activities in Canada seek to control media. ***][80] ***[81]

---

[71] CSIS, *** 2017.
[72] CSIS, *** 2017.
[73] CSIS, *** 2018.
[74] CSIS, *** 2018.
[75] See list in National Ethnic Press and Media Council of Canada, http://nationalethnicpress.com/aboutus/.
[76] CSIS, *** 2017.
[77] CSIS, *** 2017.
[78] ***
[79] Anne-Marie Brady, Discussion with Secretariat through video-conference, January 31, 2019.
[80] CSIS, *** 2018.
[81] CSE, *** March 2, 2018.

167. ***[82] This policy uses both traditional media and social media.

168. ***[83]

Efforts to control international media

169. In New Zealand, academic research suggests that the PRC has overall political control over the various Chinese media companies that own New Zealand-based Chinese-language outlets, resulting in a form of "media supervision." Over many years, PRC state media companies have invested in strategic mergers and acquisitions of Chinese-language media outlets, centralizing and controlling the messages that are available for dissemination to Chinese communities outside of the PRC.[84]

170. PRC efforts extend far beyond the short term and far beyond the West. According to *The Guardian* newspaper, the PRC's efforts also encompass

> longer-term programmes for reporters from developing countries. These moves were formalized under the auspices of the China Public Diplomacy Association, established in 2012. The targets are extraordinarily ambitious: the training of 500 Latin American and Caribbean journalists over five years, and 1,000 African journalists a year by 2020. Through these schemes, foreign reporters are schooled not just on China, but also on its view of journalism. To China's leaders, journalistic ideals such as critical reporting and objectivity are not just hostile, they pose an existential threat. . . . China's own media imperialism is on the rise, and the ultimate battle may not be for the means of news production, but for journalism itself.[85]

---

[82] CSIS, *** 2015.
[83] CSIS, *** 2016.
[84] Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities Under Xi Jinping," Paper for The Corrosion of Democracy Under China's Global Influence Conference, Supported by the Taiwan Foundation for Democracy, Arlington, Virginia, USA, September 16–17, 2017, https://wilsoncenter.org/sites/default/files/for_website_magicweaponanne-mariesbradyseptember2017.pdf.
[85] Louisa Lim and Julia Bergin, "Inside China's Audacious Global Propaganda Campaign," *The Guardian*, December 7, 2018, www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping.

Interference with academic institutions

171. Some states carry out foreign interference activities on Canadian postsecondary education campuses.[86] They seek to utilize the open and innovative features of these institutions to further their own objectives, which include interference activities but also other actions with hostile intent (e.g., espionage and intellectual property theft). Foreign interference activity seeks to influence public opinion and debate, thereby obstructing fundamental freedoms such as speech and assembly, and the independence of academic institutions. In trying to influence public debate at academic institutions, foreign states may sponsor specific events to shape discussion rather than engage in free debate and dialogue. They may also directly or indirectly attempt to disrupt public events or other activities perceived as problematic.

172. CSIS assesses that the PRC and the Russian Federation are the primary threat actors on Canadian campuses. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes Russian foreign interference activities on Canadian campuses. ***]

- ***[87]
- ***[88]

173. [*** Two sentences were revised to remove injurious or privileged information. ***][89] Academic research indicates that one such student group is the Chinese Students and Scholars Associations (CSSAs). As CSIS noted, the CSSAs are an important support mechanism for international students studying abroad and "provide a social and professional network for students . . . they are not nefarious in and of themselves."[90] However, there is growing public concern about the relationship between the associations and the PRC's embassies and consulates as the CSSAs are "one of the main means the Chinese authorities use to guide Chinese students and scholars on short-term study abroad."[91] In the United States, CSSAs are "mobilized to protest campus events that threatened to show China in a negative light. . . . Though ties with the Chinese government vary from chapter to chapter, there is reportedly 'growing ideological pressure from the embassy and consulates'. Some CSSAs already mandate loyalty to the Party line."[92] ***[93] CSSA behaviour may also pose a threat to freedom of speech and assembly. For example, a media report discussed a Toronto-based chapter of the CSSA that

---

[86] CSIS, Director, Presentation to the U15 Group, April 16, 2018.
[87] CSIS, Director, Presentation to the U15 Group, April 16, 2018.
[88] CSIS, Foreign Influence Activities in Canada, March 10, 2016.
[89] CSIS, Director, Presentation to the U15 Group, April 16, 2018.
[90] CSIS, Director, Presentation to the U15 Group, April 16, 2018.
[91] Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities Under Xi Jinping," Paper for "The Corrosion of Democracy Under China's Global Influence Conference, Supported by the Taiwan Foundation for Democracy, Arlington, Virginia, USA, September 16–17, 2017, https://wilsoncenter.org/sites/default/files/for_website_magicweaponanne-mariesbradyseptember2017.pdf.
[92] Jonas Parello-Plesnar and Belinda Li, "The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond," *Hudson Institute*, June 2018, https://s3.amazonaws.com/media.hudson.org/files/publications/JONASFINAL.pdf.
[93] CSIS, *** 2017.

immediately informed the Chinese consulate and publicly condemned a presentation at McMaster University by Rukiye Turdush, a critic of the PRC's internment of Uyghurs.[94]

174. As part of the PRC's cultural influence efforts abroad, the Chinese government funds Confucius Institutes that "teach Chinese language and culture, including calligraphy, food and dance."[95] For example, there are now more Confucius Institutes in Africa than the number of cultural centres of any other government except France.[96] In Canada, these institutes are typically affiliated with postsecondary education institutes and K–12 schools.[97] CSIS notes that New Brunswick recently shut down a Confucius Institute due to community complaints related to foreign interference.[98] In the United States, the Permanent Subcommittee on Investigations for the Committee on Homeland Security and Governmental Affairs recently completed a review of these institutes in a report entitled "China's Impact on the U.S. Education System." The report noted that,

> Confucius Institute funding comes with strings that can compromise academic freedom. The Chinese government approves all teachers, events, and speakers. Some U.S. schools contractually agree that both Chinese and U.S. laws will apply. . . . The Chinese teachers sign contracts with the Chinese government pledging they will not damage the national interests of China. Such limitations attempt to export China's censorship of political debate and prevent discussion of potentially politically sensitive topics.[99]

175. Recent Canadian media reports have highlighted similar concerns, including a January 2019 article that discussed the rejection of a Confucius Institute agreement by a Toronto school board.[100]

---

[94] Xiao Xu and Joe Friesen, "Campus disruptions lead to allegations of Chinese government interference," *Globe and Mail*, February 18, 2019.

[95] Jacques Poitras, "Confucius Institute a brainwashing program, say parents who pulled daughter from class," *CBC News*, April 8, 2019, www.cbc.ca/news/canada/new-brunswick/nb-fredericton-parents-confucius-institute-new-information-1.5086501.

[96] Geoffrey York, "China flexes its political muscles in Africa with media censorship, academic controls," *Globe and Mail*, October 9, 2018, and updated on October 11, 2018, www.theglobeandmail.com/world/article-china-flexes-its-political-muscles-in-africa-with-media-censorship.

[97] There are currently 13 Confucius Institutes in Canada, including four affiliated with K–12 school boards. Confucius Institute of Toronto website's home page. See: https://confuciusinstitutetoronto.weebly.com.

[98] CSIS, Director, NSICOP hearing, April 2, 2019.

[99] Permanent Subcommittee on Investigations for the Committee on Homeland Security and Governmental Affairs, *China's Impact on the U.S. Education System*, United States Senate, February 27, 2019, https://hsgac.senate.gov/imo/media/doc/PSI%20Report%20China's%20Impact%20on%20the%20US%20Education%20System.pdf.

[100] Tom Blackwell, "How China uses shadowy United Front as 'magic weapon' to try to extend its influence in Canada," *National Post*, January 31, 2019, https://nationalpost.com/news/how-china-uses-shadowy-united-front-as-magic-weapon-to-try-to-extend-its-influence-in-Canada; and Tom Blackwell, "Don't step out of line: Confidential report reveals how Chinese officials harass activists in Canada," *National Post*, January 5, 2019, https://nationalpost.com/news/world/confidential-report-reveals-how-chinese-officials-harass-activists-in-canada-there-is-a-consistent-pattern.

Allied institutions also under threat

176. Canada is not alone in facing the threat posed by foreign interference. Canada's close allies and some like-minded states are subject to foreign interference activities that target their respective institutions.

Australia

177. Australia appears to be at the forefront of Western nations in addressing the threat of foreign interference. In testimony to the Australian Parliamentary Joint Committee on Intelligence and Security, Australian Security Intelligence Organization officials stated that the threat from espionage and foreign interference in Australia is "unprecedented" and that it is "extensive, unrelenting and increasingly sophisticated."[101] In its 2017 Foreign Policy White Paper, the Australian government noted that it is guarding against foreign influence.

178. In discussing the threat to Australia's political leadership, China expert John Garnaut stated that:

> Reports have shown that the CCP [Chinese Communist Party] is systematically silencing critics in Australia and co-opting Chinese-language media here to present favourable views. The party is 'astroturfing' grassroots political movements to give the impression of Chinese community support for Beijing's policies and leaders, while drowning out opponents. CCP-linked organizations are crowding out independent opportunities for ethnic Chinese political representation. . . . In 2015 the Australian Security Intelligence Organization reportedly warned the major political parties that two of Australia's most generous donors had 'strong connections to the Chinese Communist Party' and that their 'donations might come with strings attached'.[102]

179. In 2017, an investigation by Four Corners and Fairfax media reported that two PRC-associated individuals donated AUS$6.7 million to the Liberal, Labour and National parties over the period of a decade.[103] The investigative series, including its reporting on the suspected influence ties between these donors and former Senator Sam Dastyari, led to increased public pressure on the Australian government to address the issue. [*** The following sentence was revised to remove injurious or privileged information. This sentence describes a memorandum from PCO to the Prime Minister. ***][104]

---

[101] Australia, Parliamentary Joint Committee on Intelligence and Security, Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, June 2018, https://aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/EspionageFInterference/Report.
[102] John Garnaut, "Australia's China Reset," *The Monthly*, August 2018, www.themonthly.com.au/issue/2018/august/1533045600/john-garnaut/australia-s-china-reset
[103] Four Corners, "ASIO warns political parties over foreign donations," *Australian Broadcasting Corporation*, June 5, 2017, https://abc.net.au/news/2017-06-05/asio-warns-political-parties-over-foreign-donations/8590162; and Four Corners, "Power and Influence," *Australian Broadcasting Corporation*, June 5, 2017, www.abc.net.au/4corners/power-and-influence-promo/8579844.
[104] PCO, *** October 2017.

180. Australia has taken a number of measures to respond. In the past 18 months, Australia has passed a suite of legislative tools to further address the threat, including the introduction of new offences in that country's *Criminal Code* in relation to espionage and foreign interference, and amendments to other offences such as treason and treachery. New provisions pertaining to foreign interference provide a high degree of specificity on offences and threat activities, including on whether the activity was in the planning stages, intentional, reckless or funded by a foreign intelligence service. The penalties range from 10 to 20 years' imprisonment.[105] The legislation creates a new transparency scheme that prescribes the registration of persons acting as agents of foreign principals and requires regular public disclosures. Australia also established a National Counter Foreign Interference Coordinator charged with delivering an "effective, efficient and consistent national response to foreign interference by providing a focal point for coordinating policy and program development and leading engagement with private sector areas."[106]

New Zealand

181. As part of the New Zealand Parliament's Justice Select's Inquiry into the 2016 and 2017 elections, the Director General of Security for the New Zealand Security Intelligence Service and the Director General of the Government Communications Security Bureau provided a briefing on foreign interference activities. During the unclassified portion of the briefing, the Director General of the Security Intelligence Service stated that "[t]he challenge of foreign interference to our democracy is also not just about what occurs around the election itself. Motivated state actors will work assiduously over many years, including in New Zealand, to covertly garner influence, access and leverage."[107] The submission also highlighted vectors of foreign interference, including cyber threats to the election, use of social and traditional media to spread disinformation, building covert influence and leverage, and the exertion of pressure on or control of diaspora communities.

182. Professor Anne-Marie Brady's internationally recognized review of PRC interference activities highlights the threat posed to New Zealand's sovereignty. Based on public and open source information, Dr. Brady's paper explains the many tools and avenues through which the PRC conducts interference activities in New Zealand, including the co-optation of individuals and members of the political class.[108]

---

[105] Australia, National Security Legislation Amendment (Espionage and Foreign Interference Act, 2018), www.legislation.gov.au/Details/CA.

[106] Australia, Department of Home Affairs, "Who we are – Our Senior Staff – Chris Teal," March 29, 2019, www.homeaffairs.gov.au/about-us/who-we-are/our-senior-staff/chris-teal.

[107] New Zealand Security Intelligence Service and Government Communications Security Bureau, Submission by Director-General of Security, NZSIS and Director General of GCSB on the Justice Committee Inquiry into the 2017 General Election and 2016 Local Election, April 11, 2019, www.parliament.nz/resource/en-NZ/52SCJU_EVI_78888_JUS67631/22077e896220070072fc5f00958ea098d1169056.

[108] Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities Under Xi Jinping," Paper for "The Corrosion of Democracy Under China's Global Influence Conference, Supported by the Taiwan Foundation for Democracy, Arlington, Virginia, USA, September 16–17, 2017, https://wilsoncenter.org/sites/default/files/for_website_magicweaponanne-mariesbradyseptember2017.pdf.

One noted example includes a member of Parliament reportedly working in the interests of a foreign state. Following the publication of her paper, Dr. Brady became the subject of targeted harassment.[109]

United States

183. The United States is also the target of foreign interference activities. The most prominent example is the extensively documented Russian foreign interference activities directed against the 2016 presidential election. On January 6, 2017, the U.S. Director of National Intelligence published a comprehensive intelligence community assessment entitled "Assessing Russian Activities and Intentions in Recent US Elections." The report found that

> Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order . . . [and that] Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.[110]

184. The United States has also been the target of PRC-led interference campaigns. In a speech on October 4, 2018, the U.S. Vice President highlighted the range of PRC threat activities directed at the United States:

> I come before you today because the American people deserve to know that, as we speak, Beijing is employing a whole-of-government approach, using political, economic, and military tools, as well as propaganda, to advance its influence and benefit its interests in the United States. China is also applying this power in more proactive ways than ever before, to exert influence and interfere in the domestic policy and politics of this country.[111]

185. The United States has employed a foreign agent registration scheme since 1938. While a recent audit of the *Foreign Agents Registration Act* presented a number of recommendations to improve its use and functions, it still requires "persons acting as agents of foreign principals in a political or quasi-

---

[109] Eleanor Ainge Roy, "'I'm being watched': Anne-Marie Brady, the China critic living in fear of Beijing," *The Guardian*, January 23, 2019, www.theguardian.com/world/2019/jan/23/im-being-watched-anne-marie-brady-the-china-critic-living-in-fear-of-beijing.

[110] United States, Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, January 6, 2017, https://dni.gov/files/documents/ICA_201701.pdf.

[111] United States, Remarks by the Vice President of the United States Mike Pence on the Administration's Policy towards China delivered on October 4, 2018, www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/.

political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts, and disbursements in support of those activities."[112]

United Kingdom

186. The United Kingdom is also the target of foreign interference activity. In testimony to the Intelligence and Security Committee in January 2017, officials from the Government Communications Headquarters briefed on Russian interference activities and noted that these are likely to continue and grow.[113] The United Kingdom recently announced a range of new measures to address electoral interference, disinformation and intimidation. On May 5, 2019, the Minister for the Constitution announced the government's commitment to introducing a new electoral offence of intimidating a candidate or campaigner during the run-up to an election, either in person or online; preparing legislation that would clarify the electoral offence of undue influence of a voter; requiring online election material to clearly indicate the individual or group that produced it; and initiating a consultation on electoral integrity, which would include strengthening laws on foreign donations.[114]

Like-minded nations

187. Beyond Canada's partners in the Five Eyes, close allies and like-minded states are also subject to foreign interference activities. For example, the Dutch General Intelligence and Security Service discussed various forms of covert and harmful foreign interference activities occurring in the Netherlands in its 2018 Annual Report. Notable concerns included Russian and Chinese political interference activities and their efforts, along with those of Iran and Turkey, to influence and intimidate ethnocultural communities.[115] The German Ministry of the Interior highlighted that Russian intelligence services deploy broad-based efforts to exercise influence, and that these services have been working at "high intensity" against German interests for many years.[116] Media reports suggest that Russian actors deployed efforts to interfere with the most recent presidential election in France, including a cyber

---

[112] United States, Office of the Inspector General, Audit of the National Security Division's Enforcement and Administration of the Foreign Agents Registration Act, U.S. Department of Justice, September 2016, https://oig.justice.gov/reports/2016/a1624.pdf.

[113] United Kingdom, Intelligence Security Committee, *ISC Annual Report 2016-2017*, December 20, 2017.

[114] United Kingdom, Cabinet Office, Government safeguards UK elections, May 5, 2019, www.gov.uk/government/news/government-safeguards-uk-elections.

[115] Netherlands, General Intelligence and Security Service, Annual Report 2018, Ministry of the Interior and Kingdom Relations, May 2019.

[116] Translated reference from the *Bundesministerium des Inneren, Verfassungsschutzbericht*, 2015, p. 254, by Constanze Stelzenmüller, a Robert Bosch senior fellow with the Center on the United States and Europe at the Brookings Institution, in testimony to the U.S. Senate Select Committee on Intelligence on June 28, 2017, www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections.

attack against French cyber infrastructure.[117] Another report stated that Russia sought to influence Marine Le Pen's far-right party with a €9.4 million loan through an obscure Russian bank.[118]

International multilateral organizations

188. International multilateral organizations are also the subject of foreign interference activities. As the U.S. Director of National Intelligence noted in the 2019 Worldwide Threat Assessment,

> China has become the second-largest contributor to the UN peacekeeping budget and the third-largest contributor to the UN regular budget. . . . Beijing has stepped up efforts to reshape international discourse around human rights, especially within the UN system. Beijing has sought not only to block criticism of its own system but also to erode norms, such as the notion that the international community has a legitimate role in scrutinizing other countries' behavior on human rights (e.g. initiatives to proscribe country-specific resolutions), and to advance narrow definitions of human rights based on economic standards.[119]

PRC efforts to interfere in the United Nations included bribes made by a PRC-linked consultant to the then President of the United Nations General Assembly.[120]

---

[117] Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election Infrastructure," *Wired*, May 9, 2017, www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure.

[118] Paul Sonne, "National Security: A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *Washington Post*, December 27, 2018. www.washingtonpost.com/world/nationa-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html.

[119] United States, Office of the Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community, presented to the Senate Select Committee on Intelligence on January 29, 2019, www.dni.gov/files/ODNI/documents/2019/ATA-SFR---SSCI.pdf.

[120] Nick McKenzie, Bethany Allen-Ebrahimian, et al., "Chinese Influence: Beijing's secret plot to infiltrate UN used Australian insider," *Sydney Morning Herald*, November 11, 2018, www.smh.com.au/world/asia/beijing-s-secret-plot-to-infiltrate-un-used-australian-insider-20181031-p50d2e.html.

The Committee's assessment of the threat from foreign interference

189. The Committee believes there is ample evidence *** that Canada is the target of significant and sustained foreign interference activities. *** The PRC, the Russian Federation *** other states ***. The Committee believes that these states target Canada for a variety of reasons, but all seek to exploit the openness of our society and penetrate our fundamental institutions to meet their objectives. They target ethnocultural communities, seek to corrupt the political process, manipulate the media, and attempt to curate debate on postsecondary campuses. Each of these activities poses a significant risk to the rights and freedoms of Canadians and to the country's sovereignty: they are a clear threat to the security of Canada.

190. Canada is not alone in facing this threat. Its closest security and intelligence allies, including those within the Five Eyes and NATO, are targeted by many of the same foreign states using many of the same techniques. Like terrorism, the threat of foreign interference is increasingly seen by states as a growing threat requiring a common response.

Part II: The response to foreign interference

191. The first part of this chapter described the breadth and scope of the threat of foreign interference. It outlined the primary threat actors, and examined the threat posed by those actors to Canada's fundamental institutions and ethnocultural communities. This part assesses the government's response to the threat, including through organizational responsibilities and activities, collaboration and coordination at various levels, and public-facing engagement. As noted in paragraph 116, the Committee's review focuses on traditional foreign interference.

192. The second part of this chapter is divided into four sections. The first provides an overview of the organizations responsible for addressing foreign interference and the tools they have at their disposal. The second examines the extent of coordination and collaboration among these organizations, using three important case studies. The third examines the degree to which the federal government has informed other orders of government, the public and fundamental institutions – all targets of foreign interference. The last section describes government engagement with allies abroad.

Overview of key responding departments and agencies

193. The Committee examined the primary security and intelligence organizations responsible for investigating and countering the threat of foreign interference as characterized by the scope of this review: CSIS, GAC, PCO, Public Safety Canada and the RCMP. The mandates, responsibilities and tools of these organizations shape how they understand and respond to foreign interference, independently or in coordination. Each of the five organizations is discussed below.

194. Other organizations play supporting roles, including CSE, in providing foreign intelligence and securing government cyber systems; Immigration, Refugees and Citizenship Canada, in determining the admissibility of individuals to enter Canada; and CBSA, in securing the border. For the purposes of this review, the Committee consulted these organizations for information, but they were not included as part of the entire review process.

Canadian Security Intelligence Service

195. Pursuant to subsection 12(1) of the CSIS Act, CSIS investigates threats to the security of Canada and provides related advice to the government. Section 2 of the *CSIS Act* defines threats to security of Canada, including: "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."[121] As previously noted, the Committee has adopted the more commonly used term of 'foreign interference' to describe this threat. CSIS's operational activities are prioritized according to the government's intelligence priorities and the assessed national security threat.[122]

---

[121] *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23, https://laws-lois.justice.gc.ca/eng/acts/c-23/page-1.html#h-2.
[122] CSIS, NSICOP: Study of Foreign Influence Activities, Presentation to NSICOP, April 2, 2019.

196. CSIS possesses a number of tools and measures to investigate and reduce threats. CSIS's intelligence collection activities may serve to advance investigations, provide advice on the admissibility of people to Canada, or to disseminate intelligence, assessments and advice to the government.[123] In carrying out investigations, CSIS may deploy a wide array of operational techniques with varying levels of intrusiveness (e.g., interviews with targets, physical surveillance, and warranted powers to intercept communications or enter premises).[124] When investigations involve Canadian fundamental institutions, CSIS policies and procedures provide specific direction, including ministerial direction, along with special considerations and enhanced approvals.[125]

197. CSIS may also use a threat reduction measure (TRM) at any stage of an investigation.[126] The *CSIS Act* defines the threshold for use of a TRM as "reasonable grounds to believe" that an activity represents a threat to the security of Canada. It also prescribes that the TRM must be reasonable and proportionate to the threat and must consider other means available.[127] [*** The following two sentences were revised to remove injurious or privileged information. The two sentences describe a CSIS policy. ***][128] ***[129]

198. CSIS devotes considerable resources to investigating and reporting on foreign interference activities. Between *** CSIS had *** targets related to espionage and foreign interference. Of these, *** targets were subject to a court warrant, which permit CSIS to use very intrusive tools and are an indication of the significance of the threat.[130] These figures include espionage and foreign interference given that hostile states will engage in both threat activities. In over four-fifths of these cases, CSIS investigations and warrants address both. In the Committee's review timeframe (January 1, 2015, to August 31, 2018), *** percent of CSIS's intelligence reports were associated with foreign interference. Comparatively,*** percent were associated with terrorism and *** percent with other activities.[131] CSIS produced *** separate intelligence assessments during the review timeframe examining the range and nature of the threat of foreign interference activity directed against Canada. These products sensitized partners and contextualized the threat ***[132]

199. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes CSIS investigative challenges. ***][133] ***[134] ***[135] During an appearance before the Committee, the Director of CSIS discussed these considerations:

---

[123] CSIS, NSICOP: Study of Foreign Influence Activities, Presentation to NSICOP, April 2, 2019.
[124] CSIS, NSICOP: Study of Foreign Influence Activities, Presentation to NSICOP, April 2, 2019.
[125] For example, such policies and procedures include ***.
[126] Subsection 12.1(1) of the *CSIS Act* enables CSIS, where it has reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, to take measures, within or outside Canada, to reduce the threat.
[127] CSIS, *** October 20, 2015.
[128] CSIS, *** October 20, 2015.
[129] CSIS, *** October 20, 2015.
[130] CSIS, RE: NSICOP: FI Review – Secondary Doc Production, June 3, 2019.
[131] CSIS, NSICOP: FI Review – Secondary Doc Production, Email to the NSICOP Secretariat, April 26, 2019; and a follow-up message in the same email chain on May 27, 2019.
[132] CSIS, NSICOP: Study of Foreign Influence Activities, Presentation to NSICOP, April 2, 2019.
[133] CSIS, *** October 13, 2017.

***[136]

200. CSIS engaged a range of other organizations and stakeholders on the nature of the threat. It held regular ongoing discussions with other federal partners, other orders of government, and some public and private institutions. At the federal level and within the review timeframe, "the Service undertook *** briefings to *** different Government of Canada clients. In addition, *** individuals from *** GoC [Government of Canada] departments attended quarterly briefings on ***[137]

201. CSIS also contributes to briefing ministers on the nature of the threat. For example, in March 2018, the Director of CSIS briefed the Acting Minister of Democratic Institutions on the overall nature of the threat.[138] CSIS regularly informs the Minister of Public Safety and Emergency Preparedness through specific briefings and CSIS's annual report to the Minister on operational activities. In 2016 and 2017, CSIS also provided general briefings or pre-travel briefings that included the topic of foreign interference to the ministers of Environment and Climate Change, Immigration, Refugees and Citizenship, Natural Resources, and Canadian Heritage and Multiculturalism.[139]

Royal Canadian Mounted Police

202. The RCMP is Canada's lead law enforcement body for national security criminal investigations. Its Federal Policing Program is responsible for conducting this work. While National Headquarters centrally coordinates national security criminal investigations, they are typically conducted by the Integrated National Security Enforcement Teams (INSETs) in Vancouver, Calgary, Edmonton, Toronto, Ottawa and Montreal and the National Security Enforcement Sections (NSES) in Fredericton, Winnipeg, Halifax and Saskatoon.[140] The Federal Policing Program has a budget of $905 million (2018–2019) from which it allocates funds for investigations.[141] The program uses a prioritization matrix to triage incoming investigative files based on the gravity of the threat to initiate investigations and allocate resources.[142] Police forces of jurisdiction may also investigate activities associated with foreign interference (e.g., harassment or intimidation), but the RCMP noted that "when these cases are confirmed to be foreign interference, the law states that they be referred to the RCMP."[143] Similar to CSIS, the RCMP has been

---

[134] CSIS, *** October 13, 2017.
[135] CSIS, *** 2017.
[136] CSIS, Director, NSICOP hearing, April 2, 2019.
[137] CSIS, *** 2019.
[138] CSIS, Director's speaking notes, Meeting with Acting Minister of Democratic Institutions, March 23, 2018.
[139] CSIS, *** 2019.
[140] RCMP, NSICOP Review – Government response to foreign interference and influence, RCMP Submission, January 10, 2019; and RCMP, NSICOP Draft Report on Foreign Interference, RCMP fact check and feedback, July 5, 2019.
[141] RCMP, NSICOP Review – Government response to foreign interference and influence, RCMP submission, January 10, 2019.
[142] RCMP, Deputy Commissioner Federal Policing, NSICOP hearing, May 2, 2019.
[143] RCMP, NSICOP Draft Report on Foreign Interference, RCMP fact check and feedback, July 5, 2019.

given direction concerning its engagement of and investigative activities involving fundamental institutions, including a Ministerial Direction on National Security in Sensitive Sectors.[144]

203. The RCMP may use various tools and measures found in statute to pursue criminal investigations and lay charges for activities associated with foreign interference. These statutes and their notable provisions include the following:

- The *Security of Information Act* establishes the offence of foreign influence: "Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign entity or a terrorist group, induces or attempts to induce, by threat, accusation, menace or violence, any person to do anything or to cause anything to be done (a) that is for the purpose of increasing the capacity of a foreign entity or a terrorist group to harm Canadian interests, or (b) that is reasonably likely to harm Canadian interests."[145] Anyone found guilty of this offence can face up to life in prison.
- The *Criminal Code* includes provisions that address treason; sabotage; interception of private communications; bribery; mischief; criminal harassment; uttering threats; extortion; false messages; indecent or harassing telephone calls; conspiracy; and intimidation.[146]

204. The *Canada Elections Act* includes an offence related to interference by non-residents in elections. Specifically, "[n]o person who does not reside in Canada shall, during an election period, in any way induce electors to vote or refrain from voting or vote or refrain from voting for a particular candidate."[147] The Act also sets out other offences associated with interfering in the conduct of federal elections in Canada. As the RCMP stated, "[t]he Commissioner of Canada Elections is the independent Officer that ensures the CEA [*Canada Elections Act*] is complied with and enforced, and may refer matters under the Act to the Director of Public Prosecutions, who decides whether to initiate a prosecution."[148]

205. The RCMP informed the Committee that, between *** and *** it identified *** foreign interference investigations. *** were classified as foreign-influenced threats to a person and another *** as foreign-influenced threats to a person or organization(s).[149] Of these, *** files were cleared by the RCMP without charges as there was insufficient evidence to proceed. *** of the cleared files *** tier 1 priority investigations, that is, highest-priority files requiring significant oversight and direction from National Headquarters.[150] The remaining *** foreign interference investigations are ongoing. The RCMP

---

[144] RCMP, Operations Manual, Chapter 12.2 National Security Criminal Investigations, July 22, 2011; and Ministerial Direction National Security Investigations in Sensitive Sectors, Original signed by the Solicitor General of Canada on November 4, 2003.
[145] *Security of Information Act*, R.S.C., 1985, C.O-5, https://laws-lois.justice.gc.ca/eng/acts/o-5/index.html.
[146] RCMP, RCMP Response to Foreign Interference – Legislative 'Tools' in Canada, July 11, 2018.
[147] *Canada Elections Act*, S.C. 2000, c. 9, https://laws.justice.gc.ca/eng/acts/E-2.01/index.html.
[148] RCMP, RCMP Efforts to Combat Foreign Interference, Briefing note to the NSIA, undated.
[149] RCMP, Additional clarification for NSICOP FI Review – May 27, May 27, 2019.
[150] RCMP, NSICOP Review: Foreign Interference and influence – RCMP Response to Secondary Document Request, Briefing note to NSICOP, March 22, 2019.

also identified an additional *** investigations in the review timeframe, though these focused on espionage rather than foreign interference.

206. Under the terms of the CSIS-RCMP One Vision framework, CSIS may disclose information and intelligence to the RCMP to initiate a criminal investigation.[151] CSIS provided the RCMP *** disclosure letters within the review timeframe. Of these disclosures, the RCMP determined that *** included no reasonable grounds to open a criminal investigation; *** was a corrected version of a previous disclosure; and ***[152]

207. The RCMP described a number of challenges *** including:

- RCMP national security operations continue to be primarily focused on counter-terrorism ***[153] ***[154]
- ***[155]
- The RCMP struggles to use intelligence provided by CSIS as evidence to support criminal investigations, where court disclosure obligations may reveal ***[156]
- ***[157]
- ***[158]

208. In characterizing its perspective of the threat, the RCMP provided investigative summaries, presentations and outreach material to the Committee. However, [*** these focused on issues unrelated to foreign interference ***][159] The RCMP also stated that "[f]oreign interference is an umbrella term under which a number of activities (such as espionage) fall across a spectrum from criminal to non-criminal."[160] For example, RCMP officials cited the case of Jeffrey Delisle, an officer of the Canadian Navy who was charged and convicted in 2013 of communicating safeguarded information to a foreign entity (Russian Federation) without lawful authority, as a clear example of foreign interference during an appearance before the Committee.[161]

---

[151] CSIS and the RCMP, CSIS–RCMP Framework for Cooperation: One Vision 2.0, November 10, 2015.
[152] RCMP, *** disclosure letters, April 15, 2019.
[153] RCMP, NSICOP Review – Government response to foreign interference and influence, RCMP submission, January 10, 2019.
[154] RCMP, Deputy Commissioner Federal Policing, NSICOP hearing, May 2, 2019.
[155] RCMP, NSICOP Review: Foreign Interference and influence – RCMP response to secondary document request, Briefing note to NSICOP, March 22, 2019.
[156] RCMP, Deputy Commissioner Federal Policing and Executive Director National Security, NSICOP hearing, May 2, 2019.
[157] RCMP, Deputy Commissioner Federal Policing and Executive Director National Security, NSICOP hearing, May 2, 2019.
[158] RCMP, Deputy Commissioner Federal Policing and Executive Director National Security, NSICOP hearing, May 2, 2019.
[159] These examples include ***
[160] RCMP, NSICOP Draft Report on Foreign Interference, RCMP fact-check and feedback, July 5, 2019.
[161] RCMP, Deputy Commissioner Federal Policing and Executive Director National Security, NSICOP hearing, May 2, 2019. In fact, Delisle was charged under sub-section 16(1) of the *Security of Information Act* for communicating to a foreign entity information that the government was taking measures to safeguard and under the *Criminal Code* for breach of trust.

Global Affairs Canada

209. GAC represents Canada's interests abroad. It manages Canada's diplomatic relations, provides consular services to Canadians, promotes the country's international trade, and leads Canada's international development and humanitarian assistance. Each bilateral and multilateral relationship is unique: depending on the partner, a bilateral relationship may include areas of cooperation, agreement, disagreement and even hostile behaviour. This requires GAC to make an ongoing calculation of complex interests and risks (e.g., trade, security, legal, political, values) when managing Canada's international relationships. [*** The remainder of this paragraph was revised to remove injurious or privileged information and to ensure readability. It discusses two countries with which Canada has important bilateral interests and which also conduct foreign interference activities in Canada. ***] In each of these cases, GAC must consider the range of its responsibilities when considering how to manage its bilateral relations.[162]

210. GAC is therefore a key player in countering foreign interference activities in Canada. When presented with evidence of interference from partners in the security and intelligence community, it must determine, usually in coordination with those partners, what tools it may use to respond. As stated by GAC officials, the objective of such measures is to "impose a cost – economic, political, reputational – to problematic behaviour in an attempt to induce behavioural change. If successful, this can deter and ultimately prevent future similar aggressive behaviour."[163] The tools or measures available to GAC are either bilateral or multilateral, including the following:

Bilateral tools

- Informally raise problematic behaviours with the country's officials;
- Formally démarche a country to raise problematic behaviours and state consequences for similar actions in the future;
- Publicly attribute a country's unacceptable behaviour;
- Reduce or suspend engagement with a country;
- Impose unilateral sanctions against a country, its officials or its proxies;
- Deny admissibility to diplomatic officials;
- Withdraw Canadian diplomatic staff; and
- Declare diplomats in Canada *personae non gratae* and have them removed.

Multilateral tools

- Coordinate diplomatic responses with like-minded states;
- Develop multilateral coalitions with like-minded partners to establish consistent and coordinated approaches to address foreign interference, including imposing multilateral sanctions; and

---

[162] With respect to *** the Deputy Minister of GAC stated, *** GAC, Deputy Minister, NSICOP hearing, April 11, 2019.
[163] GAC, Presentation to the NSICOP on Review of Foreign Interference and Influence, April 11, 2019.

- Raise a country's behaviour for consideration by international organizations.[164]

211. Determining when to respond and what tools to use is rarely easy. As GAC officials noted, "measures taken to counter foreign interference present a number of trade-offs which can impact Canada's relationships and interests . . . action is not taken in a void; any response has spillover and trade-offs."[165] Not only must GAC consider the possible implications of acting before taking measures to counter foreign interference (among other threats), it must also manage the target's response thereafter, which may include unexpected forms of retaliation and countermeasures. In characterizing the threats posed by foreign interference, a senior GAC official cited 'cyber' as the most significant form of interference.[166] This perspective is reflected in the work of GAC's Digital Inclusion Lab in 2018 and the ensuing development of the Rapid Response Mechanism.[167]

Privy Council Office

212. PCO plays a central role in government. It provides advice on matters of national and international interest; coordinates responses to issues facing the government and the country; supports the effective operation of Cabinet; and supports the development and implementation of the government's policy and legislative agendas, among other responsibilities.[168] As described in Chapter 2 of the Committee's 2018 Annual Report, within PCO the National Security and Intelligence Advisor (NSIA) plays a critical role in the areas of national security and intelligence. The NSIA is responsible for coordinating and providing leadership to the security and intelligence community, and providing advice to the prime minister, ministers and senior government officials on security and intelligence issues. Three secretariats within PCO report to the NSIA: the Security and Intelligence Secretariat, the Foreign and Defence Policy Secretariat, and the Intelligence Assessment Secretariat. These secretariats assist in coordinating the operational, policy and assessment activities of the security and intelligence community.

213. The NSIA co-chairs a number of deputy minister-level committees, including on national security and operations. These committees receive support from mirror committees at the assistant deputy minister (ADM) level (e.g., ADM National Security Policy and ADM National Security Operations). *** From an international perspective, PCO officials play an important role in engaging international

---

[164] GAC, Presentation to the NSICOP on Review of Foreign Interference and Influence, April 11, 2019.
[165] GAC, Presentation to the NSICOP on Review of Foreign Interference and Influence, April 11, 2019.
[166] Working meeting between the NSICOP Secretariat and officials from CSIS, GAC, PCO, Public Safety Canada and the RCMP, April 26, 2019.
[167] The Digital Inclusion Lab was launched in 2015 to explore issues at the intersection of digital technology and foreign policy. Much of the work presented to the Committee has focused on social media analytics and online disinformation campaigns (Digital inclusion Lab Social Media Analytics: ***). During 2018, one of its main areas of focus was digital threats to liberal democracy.
[168] PCO, "Raison d'être, mandate and role: who we are and what we do," April 3, 2019, www.canada.ca/en/privy-council/corporate/mandate.html.

partners on security and intelligence issues. For example, PCO is the lead Canadian organization at the ***[169]

214. During the review period, PCO provided or supported briefings on the issue of foreign interference to various Cabinet ministers. With regard to the Prime Minister, PCO provided five briefings on specific threat activities occurring in Canada, including on ***[170] In an appearance before the Committee, the NSIA also spoke to the more recent roles and responsibilities of supporting the new Minister of Democratic Institutions.[171] For example, PCO officials provided the Minister of Democratic Institutions a preliminary in-person briefing on foreign electoral interference (i.e., threats to elections in other countries) and hostile state activity in January 2018, and a three-page summary of intelligence assessments on foreign interference in the spring of 2018.[172]

215. In addition to PCO's support to the Prime Minister and Minister of Democratic Institutions, the NSIA briefed the *** Ministers of Public Safety and Emergency Preparedness, Foreign Affairs, and National Defence ***[173] Also of note, the NSIA briefed the Minister of Foreign Affairs on foreign interference prior to international travel in January 2017.[174]

216. PCO recently started coordination activities on the development of policy approaches, including two policy papers describing "hostile state activity." PCO defines hostile state activity as "activities carried out by foreign states (and/or associated non-state actors) to influence or interfere in the political, economic and security affairs of Canada through overt or covert means."[175] While the review will cover interdepartmental coordination in greater depth in the forthcoming section, PCO started to focus its attention in early 2018 on coordinating the government's response to foreign interference. For example, records from two meetings of the Deputy Minister National Security Committee (September 2017 and March 2018) show very preliminary conversations on the need to develop a government-wide approach to foreign interference. PCO also continued to *** where foreign interference has been identified as a government-wide priority for the past few decades.

---

169 ***

170 In the review period, PCO submitted the following briefing notes to the Prime Minister of Canada on foreign interference–related issues: *** November 2018; *** June 29, 2017; *** October 17, 2017; *** January 2018; and *** October 2017.

171 PCO, NSIA, NSICOP hearing, April 30, 2019.

172 PCO, Threats and Risks to Democracy: An Intelligence Perspective, June 7, 2018.

173 *** PCO could not confirm the exact dates of these respective briefings.

174 The following note was provided by CSIS, though the briefing was delivered by the NSIA: CSIS, NSIA briefing to Global Affairs Minister, January 31, 2017.

175 PCO, HSA [Hostile State Activity] Overview, October 2017.

Public Safety Canada

217. In supporting the responsibilities of the Minister of Public Safety and Emergency Preparedness, Public Safety Canada exercises three roles:

- support the Minister's responsibility for all matters related to public safety and emergency management not assigned to another federal organization;
- exercise leadership at the national level for national security and emergency preparedness; and
- support the Minister's responsibilities for the coordination of entities within the Public Safety portfolio.[176]

218. Public Safety Canada has only recently identified and dedicated specific resources to the issue of foreign interference. These resources contributed to the community's broader work on hostile state activity.[177]

[176] Public Safety Canada, "About Public Safety Canada," March 11, 2019, www.publicsafety.gc.ca/cnt/bt/index-en.aspx.
[177] Public Safety Canada, Overview of Public Safety Resources Dedicated to Hostile State Activity, January 16, 2019.

Interdepartmental coordination

219. As discussed in Part I of this review, the threat to Canada from foreign interference is increasing. The perpetrators have become more brazen and their activities more entrenched. While the tools at the government's disposal to fight or counter foreign interference and to mitigate it through transparency are organization- and activity-specific, the size and scope of the threat from foreign interference requires a coordinated and informed response. In a briefing to the government's Executive Leadership Development Program, the Director of CSIS stated that the government "must . . . seek to respond from a whole-of-government perspective, which requires cooperation across several government departments, some who may have competing priorities and mandates."[178] This section examines the extent to which the security and intelligence community works in concert.

220. Over the course of the period under review, the government's approach to coordination on foreign interference evolved. Up until mid to late 2017, interdepartmental coordination and collaboration on foreign interference was issue-specific and ad hoc. In general, the department or agency that was the most implicated or had the most information on a specific incident of foreign interference was the organization to lead on the coordination of response. ***

> [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes high-level considerations. ***][179]

221. PCO's depiction is reflected in the records of the ADM national security committees, which show few discussions of issue-specific incidents or challenges. It is also reflected in two committees struck specifically to deal with discrete incidents of foreign interference: the *** committee to address the PRC's efforts to repatriate so-called economic fugitives and the *** committee on the Canadian response to Russian Actions. These are discussed in case studies (paragraphs 228-254).

222. By late 2017, the community recognized that it needed better coordination to respond effectively to foreign interference. In a background memo for the *** Meeting on *** the RCMP noted that:

> There are currently a number [of] inter-related . . . initiatives/working groups including, but not limited to: Hostile State Actors; Protecting Democratic Institutions; and Economic Security. It has been identified that this is becoming burdensome, and that groups may not be appropriately leveraging discussions underway in other fora.[180]

---

[178] CSIS, Director, *** 2018.
[179] PCO, *** October, 2017.
[180] RCMP, *** May 11, 2018.

223. In March 2018, the Deputy Ministers of National Security attended a retreat to discuss hostile state activity.[181] In his opening remarks, the NSIA noted that hostile state activity ***[182]

224. In preparation for the retreat, PCO provided participants with a background paper. It noted that:

> [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes considerations. ***][183]

225. The security and intelligence community identified areas it needed to address for Canada to be more effective in countering foreign interference. These included:

- prioritizing those sectors and areas of concern that are most important to Canada and Canadian interests;
- better educating the public;
- ***
- ***
- ***
- ***[184]

226. Work in this regard is in the early stages. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes several measures that were put in place. ***][185] ***[186]

227. Table 12 lists the interdepartmental committees working on hostile state activities during the period under review.

---

[181] Deputy Ministers and Agency Heads from: PCO, Public Safety Canada, Justice, Transport, Innovation, Science and Economic Development Canada, the RCMP, CBSA, Financial Transactions and Reports Analysis Centre, GAC, Finance, Department of National Defence / Canadian Armed Forces, CSIS, and Immigration, Refugees and Citizenship Canada.
[182] PCO, *** March 2018.
[183] PCO, Countering Hostile State Activity: The Canadian Perspective, March 2018.
[184] PCO, *** March 2018.
[185] PCO, DGHSA [Director General Hostile State Activity] Working Group Meetings, Calendar invitations, May 24, 2018; June 5, 2018; July 6, 2018; and August 7, 2018.
[186] Public Safety Canada, Workplan – Hostile State Activities, June 14, 2018.

Working Group	Lead Organization	Participants	Format	Status
ADM Committee on Protecting Canada's Democracy	PCO	PCO, CSE, CSIS, Canadian Heritage, Innovation, Science and Economic Development Canada, GAC, Department of Justice, RCMP, DND, Financial Transactions and Reports Analysis Centre (FINTRAC), Treasury Board Secretariat, Public Safety Canada	ADM-level interdepartmental working group	Commenced ***
ADM Electoral Security Steering Committee	PCO and Elections Canada	CSE, CSIS, GAC, RCMP, PS	ADM-level interdepartmental working group	Commenced ***
ADM Working Group ***	GAC	PCO, CSIS, CSE, PS, RCMP, DND, Finance, FINTRAC, CBSA, IRCC, Transport Canada	ADM-level interdepartmental working group	Commenced ***
Director General Working Group on Hostile State Activity	PCO and Public Safety Canada	GAC, CSIS, CSE, RCMP, DND/CAF, PCO-Democratic Institutions	Director General–level interdepartmental working group	Commenced ***
Inter-departmental Working Group on Hostile State Activity	Public Safety Canada and PCO	PCO, CSE, DND, RCMP, GAC, CSIS, Public Safety Canada, FINTRAC, CBSA	Director-level interdepartmental working group	Commenced ***
Hybrid Threats Inter-departmental Working Group	GAC, Public Safety Canada and DND	PCO, CSE, DND, RCMP, GAC, CSIS, CBSA	Director-level interdepartmental working group	Commenced ***

Source: PCO, ***, August 2018 and a PCO follow-up email on August 28, 2019.

Table 12: Inventory of Government of Canada Interdepartmental Working Groups on Hostile State Activities

Case studies of Canadian responses to instances of foreign interference in Canada

228. The Committee examined the measures Canada took to address foreign interference activities in three instances during the course of the period under review (January 1, 2015, to August 31, 2018). In each case, the activities were long-standing and part of a broader range of hostile activities detrimental to Canadian interests. These cases involve *** foreign interference threats to Canada: PRC, the Russian Federation and *** They demonstrate in concrete terms the roles played by organizations in the security and intelligence community, the challenges they face in responding to threats and coordinating their own activities, and the considerations that went into deciding if, when and how to act.

China and its Operation Fox Hunt

229. Since coming to power in late 2012, Chinese president Xi Jinping has made fighting government corruption a cornerstone of his policy to re-establish the legitimacy of the CCP. This policy resulted in significant changes to China's machinery of government, refocused the work of its security and police apparatus, and has proven politically popular.[187] A key part has been a campaign to track down and return allegedly corrupt individuals (economic fugitives) who had fled abroad, most commonly to Canada, the United States and Australia.[188] Known as Operation Fox Hunt (later, Sky Net), this campaign is important for President Xi to demonstrate to the Chinese people the CCP's sincerity in cleaning up government corruption.[189]

230. Chinese security officials have taken a number of measures to conduct Operation Fox Hunt, including diplomatic pressure on foreign states to cooperate with their investigations and covert trips to persuade or coerce fugitives to return.[190] They employ these measures with Canada. On a diplomatic level, Chinese police and prosecutors work with the RCMP to arrange to meet fugitives in Canada, ostensibly to gather evidence and to discuss the case against them. Chinese authorities agree to seek permission from the RCMP prior to travelling to Canada and to abide by the terms of the *Protocol on Foreign Criminal Investigators in Canada,* including that meetings are held in RCMP facilities and monitored by an RCMP officer.[191] [*** The remainder of this paragraph was revised to remove injurious or privileged information. It discusses Chinese tactics. ***][192] ***[193]

---

[187] Tom Phillips, "China launches global 'fox hunt' for corrupt officials: Beijing vows to drive corrupt officials from their overseas refuges in a bid to save the Chinese Communist Party from extinction," *Telegraph* (U.K.), July 25, 2014.

[188] As part of Fox Hunt, the PRC posted a list of China's top 100 most wanted, 26 of whom were reportedly in Canada. Nathan Vanderklippe, "China's Fox Hunt in Canada strains trust that an extradition treaty is possible," *Globe and Mail*, September 23, 2016.

[189] In some instances, Fox Hunt is also likely used by President Xi to eliminate political rivals by returning fugitives who will provide evidence to build a case of corruption against senior members of the CCP.

[190] See, for example, Mark Mazzeti and Dan Levine, "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; and Zach Dorfman, "The Disappeared: China's global kidnapping campaign has gone on for years. It may now be reaching inside U.S. borders," *Foreign Policy*, March 29, 2018.

[191] RCMP, Protocol on foreign criminal investigators in Canada, www.rcmp-grc.gc.ca/en/protocol-foreign-criminal-investigators-canada.

[192] CSIS, ***, various dates.

231. A number of organizations responded to Operation Fox Hunt based on their respective mandates. In 2015, GAC took the lead ***[194] GAC established an interdepartmental working group with CSIS, the RCMP, the Department of Justice and CBSA that met regularly (every two to three months) to discuss Fox Hunt.[195] ***[196]

232. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes the objectives of one government department in attending coordination meetings. ***][197]

233. The RCMP worked with Chinese officials to support their investigations of corrupt officials. RCMP officials obtained information to substantiate the allegations against the alleged fugitives, facilitate Chinese requests to travel to Canada to interview the individuals and, in Canada, monitor the interviews. The RCMP imposed increasingly stringent criteria on PRC investigators as time passed. [*** The remainder of this paragraph was revised to remove injurious or privileged information. It describes challenges raised by the RCMP. ***][198]

234. [*** Paragraphs 234 and 235 were revised to remove injurious or privileged information. These paragraphs describe various government measures to address Chinese Fox Hunt activities.***][199] ***[200] ***[201]

***[202]

235. ***

236. Despite these interventions, Chinese *** activities to advance Operation Fox Hunt continued. [*** The remainder of this paragraph was revised to remove injurious or privileged information. It describes a specific instance of covert foreign interference.***][203] No action was taken at that time or, more generally, since.

---

[193] CSIS, *** 2018.
[194] GAC, Government of Canada *** June 19, 2015.
[195] GAC, Interdepartmental Meeting on Fugitives, May 11, 2016.
[196] GAC, Assistant Deputy Minister (ADM), NSICOP Secretariat meeting with the security and intelligence community, April 26, 2019.
[197] GAC, Interdepartmental Meeting on Fugitives, May 11, 2016.
[198] RCMP, NSICOP Secretariat meeting with the security and intelligence community, April 26, 2019.
[199] GAC, WJGR 0090 Report on JFM June 23-24 Trip to Beijing, June, 2015.
[200] *** CSIS, *** 2016.
[201] GAC, *** Nov. 14, 2016, Email, October 26, 2016.
[202] GAC, *** November 14, 2016.
[203] GAC, *** November 20, 2017.

237. [*** Paragraphs 237 and 238 were revised to remove injurious or privileged information. The paragraphs describe CSIS communications with a number of government departments about challenges in addressing Fox Hunt activities. ***]

***[204]

238. ***[205]

239. [*** This paragraph was revised to remove injurious or privileged information. The paragraph describes a briefing note to the Prime Minister. ***][206]

240. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes how Interdepartmental coordination on Fox Hunt appears to have waned. ***][207] ***[208]

[204] CSIS, *** 2018.
[205] CSIS, *** March 5, 2018.
[206] PCO, *** November 2018.
[207] CSIS, *** NSICOP Secretariat meeting with the security and intelligence community, April 26, 2019.
[208] CSIS, *** NSICOP Secretariat meeting with the security and intelligence community, April 26, 2019; and CSIS, *** 2018.

Russia and the Salisbury incident

241. As discussed in the first part of this chapter, the Russian Federation has conducted foreign interference activities in Canada *** The objectives of its activities include advancing its geopolitical interests, ensuring regime legitimacy and survival, countering the policies and interests of Western states, and weakening democratic institutions. [*** The rest of this paragraph was revised to remove injurious or privileged information. It discusses Russian tools of interference. ***]

242. On March 4, 2018, former Russian spy Sergei Skripal and his daughter, Yulia, were found unconscious on a park bench in Salisbury, United Kingdom. A British investigation revealed that they had been poisoned by a nerve agent smeared on their front door by Russian intelligence agents. President Vladimir Putin denied any Russian involvement in the incident. On March 20, the United Kingdom expelled 23 Russian diplomats and their families.[209] During this period, ***

243. GAC was the principal organization responsible for providing options to respond to Russia's behaviour. In response to a request from the United Kingdom for solidarity in addressing Russia's problematic behaviour,[210] [*** The rest of this paragraph was revised to remove injurious or privileged information. It discusses advice given by GAC officials to the Minister of Foreign Affairs. ***][211]

244. Following a formal request from the United Kingdom to expel Russian diplomats on March 23, 2018, the Minister of Foreign Affairs released a March 26 statement announcing the expulsion of four Russian diplomats from Canada and the denial of an application for three additional Russian diplomatic staff. The Minister stated that the four diplomats were "intelligence officers or individuals who have used their diplomatic status to undermine Canada's security or interfere in our democracy." The Minister called the poisoning "part of a wider pattern of unacceptable behaviour by Russia" and stated that "Canada fervently supports the measures that the United Kingdom has taken so far and remains resolutely committed to acting in concert with its allies."[212] Ultimately, 29 countries expelled a total of 145 Russian officials.[213]

245. Security and intelligence organizations considered the Salisbury incident in a number of interdepartmental fora. The ADM Committee on National Security Operations was scheduled to discuss the incident on March 20 as part of a wider agenda. The agenda item included two parts: a presentation

---

[209] BBC News, "Russian spy poisoning: What we know so far," *BBC*, October 8, 2018, www.bbc.com/news/uk-43315636.
[210] United Kingdom, Parliament, House of Commons Debates, 57th Parliament, 1st Session, Volume 637, March 14, 2018; Patrick Wintour, et al., "Russian spy attack: PM prepares reprisals as deadline passes," *The Guardian*, March 14, 2018, www.theguardian.com/politics/2018/mar/13/russian-spy-attack-trump-supports-uk-all-the-way; and Patrick Wintour, "UK's effort to rally allies over Sergei Skripal poisoning may fall short," *The Guardian*, March 13, 2018, www.theguardian.com/uk-news/2018/mar/13/sergei-skirpal-poisoning-russia-uk-sanctions-eu-lack-consensus.
[211] GAC, Note to the Minister of Foreign Affairs *** March 23, 2018.
[212] GAC, Canada expels Russian diplomats in solidarity with United Kingdom, Press statement, March 26, 2018.
[213] Prime Minister of Canada, Joint Statement by the Leaders of France, Germany, the United States, Canada and the United Kingdom on the Salisbury Attack, September 6, 2018. The leaders stated that they had "taken action together to disrupt the activities of the GRU [Russian intelligence] through the largest ever collective expulsion of undeclared intelligence officers."

by the RCMP and the Canadian Armed Forces on how the government would respond to an attack using chemical, biological, radiological or nuclear material inside of Canada, ***[214]

246. In early April 2018, GAC convened a *** group on Russia that continued meeting through June of that year. Participation consisted of a core group of officials from *** and a secondary group of officials from *** [*** The rest of this paragraph was revised to remove injurious or privileged information. The paragraph describes the objectives of the interdepartmental meeting. ***][215]

247. In June 2018, the *** Interdepartmental Meeting on Potential Canadian Responses to Russian Actions became the *** Interdepartmental Meeting on Canadian Responses to Hostile State Activities. The focus of the group was expanded beyond Russia to begin dealing with the G7 Rapid Response Mechanism and mapping of hostile state activities, both of which will be discussed later in this review.[216] The Committee has no information that this group met after its initial June 2018 meeting.

---

[214] The Privy Council Office neither confirmed nor denied that these discussions occurred. PCO noted that, "Records of decision or meeting minutes are not typically produced for ADM NS Ops [national security operations] meetings. Proposed speaking points contained in the Annotated Agendas submitted by PCO are not a confirmation that the topic was discussed in general or that the Assistant Secretary to the Cabinet, Security and Intelligence, raised the specific points suggested." ADM Committee on National Security Operations, Annotated Agenda, March 20, 2018.

[215] GAC, *** August 15, 2018.

[216] GAC, *** Interdepartmental Meeting on Potential Canadian Responses to Russian Actions, Minutes, June 20, 2018.

***

248. [*** Paragraphs 248 to 254 were revised to remove injurious or privileged information. The paragraphs describe a government response to a specific country which had conducted foreign interference activities in Canada. ***][217]

249. ***

- ***
- ***
- ***
- ***
- ***[218]

250. ***[219]

251. ***[220]

252. ***[221] ***[222]

253. ***

254. ***[223] ***[224]

---

[217] ***
[218] CSIS, *** 2016.
[219] CSIS, *** April 26, 2019.
[220] CSIS, *** July 31, 2015.
[221] CSIS, *** 2017.
[222] PCO, *** June 29, 2017.
[223] ***
[224] CSIS, *** October 17, 2017.

Intergovernmental and public engagement

255. Informing vulnerable institutions and the public can help to build resiliency against foreign interference. Actors within civil society and non-federal levels of government are frequent targets of foreign states' hostile activities, *** This section examines the government's efforts to engage these actors.

Intergovernmental engagement

256. PCO holds the federal portfolio for intergovernmental relations. During the period under review, PCO officials engaged in limited and ad hoc domestic engagement and outreach on the issue of foreign interference. In a four-month window in 2017, the NSIA attended the Federal, Provincial and Territorial Clerks and Cabinet Secretaries Meeting to brief on national security issues. In discussing foreign interference during the April meeting, the NSIA delivered a Secret-level presentation that provided preliminary information on threats and mitigation measures for the leaders of Canada's various bureaucracies. During the July meeting with the same audience, the NSIA used many of the same talking points.[225]

257. In April 2018, the Ontario Security Advisor organized a conference for provincial security advisors entitled "Global Threats, Local Impacts: Provincial Security Matters." The NSIA delivered the keynote address and highlighted a number of high-level security concerns associated with foreign interference, including threats to democratic institutions, the targeting of diaspora communities, and the need to increase domestic collaboration.

258. Public Safety Canada is responsible for supporting the Federal, Provincial and Territorial Meetings of Ministers Responsible for Justice and Public Safety. The issue of foreign interference was not brought forward for federal, provincial and territorial consideration at any point in the review timeframe. Public Safety Canada provided no other material associated with any outreach or engagement activities.

259. CSIS conducts significant outreach to non-federal governments and organizations on the range of threats to Canada. These activities are widespread and are led by all levels of the organization, including by the Director, and carried out across all regions of the country. However, CSIS's engagement with the public appears to be ad hoc. Depending on priorities, investigations and capacity, each region engages institutions within their jurisdiction. There is no consistent strategy to identify organizations for engagement. For example, CSIS briefed [*** a specific municipality in 2018 ***] but has no formalized plan to engage other municipalities or orders of government in Ontario or elsewhere.

260. Additionally, CSIS primarily shares general information on foreign interference outside of the federal government. These meetings and briefings typically provide an overview of CSIS's mandate, key

[225] PCO, NSIA Remarks to PTs [Provinces and Territories], April 2017 and July 2017.

threats to the security of Canada or pre-travel briefings, with a cursory discussion of foreign interference. [*** This sentence was revised to remove injurious or privileged information. This sentence describes a CSIS brief to officials of a province and notes the scarcity of information in a presentation on foreign interference. ***][226] Similar text is found in many of the other briefing and outreach documents.

261. CSIS is limited in the quantity and depth of information it can share due to the sensitivity of the issue and the classification of material. Many of the other organizations meeting with CSIS, most notably representatives from other orders of government, do not have the necessary security clearance to see classified material. Where the ability to engage at a classified level exists, CSIS has provided more detailed briefings to key partners. [*** This sentence was revised to remove injurious or privileged information. This sentence describes a CSIS brief to officials of a province and notes that significant information was provided on foreign interference. ***][227]

262. The RCMP's coordination and outreach activities on foreign interference are preliminary. In an August 2018 briefing note to the NSIA, the RCMP highlighted future opportunities for domestic partner coordination and engagement:

> The RCMP is in a unique position to facilitate Government of Canada efforts to combat FAI [foreign actor interference]. For example, citizens would likely report acts of intimidation to local law enforcement, which allows the RCMP and its police of jurisdiction partners to investigate and potentially disrupt the activity, and also to report such activities to the broader security and intelligence community. The RCMP can also engage in proactive prevention activities by helping inform industry and academia of potential vulnerabilities, and building strong relationships with diaspora communities. The RCMP is engaging with the Canadian Association of Chiefs of Police (CACP) to help inform POJs [police of jurisdiction] of the threat, and establish mechanisms for reporting incidents.[228]

263. The RCMP organized a foreign interference workshop with select domestic law enforcement partners in March 2019. The RCMP's post-event summary notes that "[a]cross all of the discussions, one clear area for further work emerged – a need to raise awareness of [foreign actor interference] with frontline police. Participants communicated that, in general, police either have not heard of [foreign actor interference], or vaguely understand it."[229] However, much of the information delivered to domestic law enforcement at this workshop characterized the threat as both foreign interference and espionage.

---

[226] CSIS, *** August 31, 2017.
[227] CSIS, *** January 12, 2016.
[228] RCMP, RCMP Efforts to Combat Foreign Interference, Briefing note to the NSIA, August 15, 2018.
[229] RCMP, Foreign Actor Interference (FAI) Workshop Notes, Post-event summary notes for the Deputy Commissioner Federal Policing, May 6, 2019.

264. The RCMP also raised the threat of foreign interference with the Canadian Association of Chiefs of Police (CACP). In 2018, the RCMP outlined a starting point for a coordinated domestic approach by law enforcement: "The RCMP continues to examine how to improve its ability to responds [sic] to the threat of foreign interference. As these efforts continue, CACP members are asked to report incidents of potential foreign interference to Federal Policing. . . . This would enhance our collective understanding of the magnitude and scope of this threat and assist in the development of mitigation strategies in the future."[230]

Public engagement

265. The Minister of Democratic Institutions has spoken publicly about the government's efforts to safeguard the 2019 election.[231] In January 2019, together with the Ministers of Public Safety and Emergency Preparedness and National Defence, the Minister of Democratic Institutions announced a plan to combat foreign interference; strengthen organizational readiness; encourage social media platforms to act; and enhance citizen preparedness. The announcement included a statement that key members of national political campaigns will now receive "regular security briefings including classified information on the foreign interference activities both cyber and human that target Canadian democratic institutions."[232] While the Committee's review excludes efforts to safeguard the 2019 federal election, the Committee received no information from PCO on initiatives to engage political parties as it relates to the review's scope more generally. In that context, the Committee highlights its recommendation from the Special Report on the Prime Minister's February 2018 trip to India, which stated that "[i]n the interest of national security, members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada."[233]

266. CSIS also conducts public outreach. In April 2018, the Director spoke to the U15, a group of some of Canada's most research-intensive universities on threats facing their campuses. Because these remarks were unclassified they represent the most public discussion and articulation of the threat, including attribution of threat actors, of foreign interference reviewed by the Committee. For example, the Director's remarks highlighted that:

> Certain foreign intelligence services and government officials (especially those of China and Russia), are also involved in the monitoring and/or coercion of students, faculty and other university officials. In some instances, students are pressured to

---

[230] RCMP, Canadian Association of Chiefs of Police [CACP] 2018 Summer Report, Draft input to the CACP, July 20, 2018.
[231] The Minister of Public Safety and Emergency Preparedness delivered a speech on national security to the Empire Club of Canada in December 2018 and a very similar speech to the Johnson Shoyama Graduate School of Public Policy in January 2019. The Minister highlighted general instances of hostile state activity, including foreign interference, along with recent domestic and international efforts to address the issue (e.g. the *Elections Modernization Act* and the Rapid Response Mechanism, both of which the Committee discusses later in the chapter).
[232] PCO – Democratic Institutions, The Government of Canada's Plan to Safeguard Canada's 2019 Election, January 30, 2019.
[233] NSICOP, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, December 3, 2018.

> participate in activities (e.g., demonstrations, spying on other students, etc.) which are covertly organised by a foreign power to further its political influence. Universities can also be used as venues for "talent-spotting" and intelligence collection, in specific circumstances . . . [and] Chinese threat actors have aggressively engaged in foreign influenced activities in Canada, as they have in Australia, the United States, and New Zealand.[234]

The Assistant Director of Intelligence delivered similar remarks to York University in June 2018. In December 2018, the Director of CSIS delivered a speech to the Economic Club of Canada in which he provided an overview of Canada's threat environment, including a description of the threat posed by other states to Canada's democratic systems and institutions.[235]

267. CSIS is increasingly preparing unclassified material drawing on open source information to further expand these briefings;[236] however, in the Canadian context, there is a shallow pool of publicly available information. In addressing this gap, CSIS's Academic Outreach Branch has held a number of workshops and expert briefings with academics, representatives from numerous federal departments and agencies, and other international experts. The Branch published two reports from workshops during the period under review that considered foreign interference: *Rethinking Security: China and the Age of Strategic Rivalry* and *Who Said What?: The Security Challenges of Modern Disinformation*.

---

[234] CSIS, Director presentation to the U15 Group, April 16, 2018.
[235] CSIS, "Remarks by David Vigneault at the Economic Club of Canada," December 4, 2018, www.canada.ca/en/security-intelligence-service/news/2018/12/remarks-by-director-david-vigneault-at-the-economic-club-of-canada.html.
[236] Working meeting between the NSICOP Secretariat and officials from CSIS, GAC, PCO, Public Safety Canada and the RCMP, April 26, 2019.

International collaboration and coordination

268. Canada and its allies have started to examine ways they can develop comprehensive and multilateral strategies to identify and counter the threat of foreign interference. During Canada's most recent G7 presidency in June 2018, leaders collectively articulated the principled footings among economic partners to address foreign interference:

> The G7 share common democratic values of respect for fundamental freedoms, human rights and the rule of law. We are committed to a rules-based international order, which is central to the maintenance and development of free, open, well-governed, pluralistic, peaceful, and prosperous societies, together with cooperation and security among states. Foreign actors seeking to undermine democratic institutions and processes through coercive, corrupt, covert or malicious means constitute a strategic threat, which we commit to confront together, and with other countries that share democratic values. Effectively responding to this threat will require a coordinated, multi-dimensional approach that respects human rights and fundamental freedoms and is developed in consultation with government and non-government stakeholders, including civil society and the private sector. . . . We commit to exchange information, coordinate action and develop strategies to reinforce our democracies and strengthen our societies' resilience.[237]

269. In support of this commitment, G7 leaders announced a "Rapid Response Mechanism" at the G7 Summit in June 2018, which was conceptualized during the Foreign and Security Ministers Meeting of the G7 in April 2018 in Toronto. The Rapid Response Mechanism's purpose is to "strengthen national and international capacities to work in a coordinated manner to reinforce our democracies, strengthen our societies' resilience and uphold freedom of expression and a free and independent media."[238] The Rapid Response Mechanism's primary mandate is to monitor, identify and compile information on foreign interference, coordinate efforts, actively share information, and identify opportunities for action.[239] GAC noted that like-minded nations could also be added to the Rapid Response Mechanism, and that the Netherlands, Australia and New Zealand had been added recently.[240]

270. Members of the Five Eyes have collectively recognized the threat posed by foreign interference throughout the alliance. In August 2018, the Five Eyes ministers of Public Safety, Immigration and Justice collectively announced their intention to collaborate in countering foreign interference:

> We agreed to draw upon the strengths of our cohesive societies, our public and private institutions, and our global partnerships to reduce the risk that foreign interference poses to domestic and global prosperity and stability. We committed to

---

[237] GAC, G7: Defending Democracy – Addressing Foreign Threats, June 2018.
[238] GAC, G7 Rapid Response Mechanism, April 2018.
[239] GAC, G7 Rapid Response Mechanism, April 2018.
[240] GAC, ADM of International Security and Political Affairs, NSICOP hearing, April 11, 2019.

> establish a mechanism for the five countries to share developments in our respective approaches to confronting the foreign interference challenge. We undertook to share information on foreign interference activities with a view to advancing our collective knowledge of how to counter such threats. In the event of a severe foreign interference incident within our sovereign nations we agreed the five countries would coordinate on appropriate responses and attribution.[241]

271. These high-level commitments inform the international engagement by Canada's security and intelligence community. [*** This sentence was revised to remove injurious or privileged information. This sentence describes an example of CSE and CSIS international engagement. ***][242]

272. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes PCO international engagement. ***]

- ***
- ***
- ***
- ***[243]

273. The RCMP has also started contributing to the international law enforcement dialogue on foreign interference. [*** This paragraph was revised to remove injurious or privileged information. This paragraph describes an instance of RCMP international engagement. ***]

> ***[244]

274. In addition to supporting the government's efforts on G7 commitments and implementing the Rapid Response Mechanism, working-level officials from GAC contributed to a coalition of like-minded states on addressing the *** Countries in this forum shared information on specific cases of ***[245] Working-level officials also contributed to issue-specific meetings with like-minded states. Representatives from GAC, the RCMP and the Department of Justice attended a June 2018 meeting organized by the U.S. State Department with like-minded nations to examine institutional vulnerabilities and areas of collaboration (e.g., political, media, education, law enforcement).[246] Notable commitments from this meeting included an agreement to share information, tools and *** engagement strategies.[247]

---

[241] Australia, Department of Home Affairs, "Five Country Ministerial 2018 – Official Communiqué," www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018.
[242] CSE, *** Conference 2018: Final Report, July 2018.
[243] PCO, *** May 2018.
[244] RCMP, *** June 19, 2018.
[245] GAC, Human Rights Exchange Meeting, Report, January 2018.
[246] GAC, *** August 13, 2018.
[247] GAC, *** August 13, 2018.

The Committee's assessment of the response to foreign interference

275. As it responds to all threats to its national security, Canada takes measures to protect itself from the threat of foreign interference. A number of organizations within the security and intelligence community have specific mandates and tools to investigate and counter this threat. They coordinate their activities through established interdepartmental mechanisms and engage sub-national levels of government, the public and like-minded states to advance key policy objectives. The Committee provides its assessment of each of these activities below.

Differences in how the threat of foreign interference is understood

276. Security and intelligence organizations do not share a common understanding of the threat, including its gravity in Canada and its most common manifestations. Over the years, CSIS has investigated foreign interference and provided other government organizations with numerous assessments on the aggressive and pervasive nature of the threat in Canada. [*** The following two sentences were revised to remove injurious or privileged information. They describe CSIS assessments of foreign interference in Canada. ***][248] ***[249] Despite these clear and consistent assessments, there are differences in how key organizations, such as PCO and the RCMP, understand the threat from foreign interference.[250]

277. Another key challenge is differences in definitions. While the *CSIS Act* defines and distinguishes between foreign influence and espionage as separate threats to the security of Canada, section 20 of the *Security of Information Act* does not make such a distinction.[251] This is most significant for the RCMP, the organization responsible for conducting criminal investigations of foreign interference. In its documentation and appearance before the Committee, the RCMP does not distinguish between espionage and foreign interference. The Committee recognizes that hostile foreign states will engage in both espionage and foreign interference, but it also notes that there is a clear distinction between espionage (i.e., exfiltration or stealing of information) and foreign interference (i.e., use of clandestine means or threats to promote a certain position or objective). While from a criminal investigation perspective the difference may not be essential, it is essential to establishing a common understanding and response to the threat from an interdepartmental perspective. As Michael Cole notes:

> Sharp power activities such as co-optation, censorship and disinformation are undoubtedly unethical, but our legal systems are ill-equipped to address those. Those activities therefore fall between the cracks in our systems, leaving law

---

[248] CSIS, various document and dates. ***

[249] CSIS, *** June 15, 2018.

[250] At an April 30, 2019, Committee hearing, a senior PCO official stated that Canada *** At that same hearing, the NSIA devoted the majority of her remarks to *** A scenario note prepared for the RCMP Deputy Commissioner of Federal Policing stated, ***

[251] No one has ever been charged under section 20 of the *Security of Information Act*.

enforcement, counterintelligence agencies, and the courts at a loss as to jurisdictions.[252]

278. Another issue is the prominence that 'cyber' has taken as a form of interference. There is little doubt that cyber threats, including the use of cyber means to conduct interference, have become both publicly known and increasingly important to the protection of government operations and private networks. In that context, the Committee notes the substantial investments in CSE cyber security operations, the implementation of measures to protect the 2019 federal election, and the creation of specific organizational units, such as the Rapid Response Mechanism Coordination Unit at GAC. The *Elections Modernization Act* seeks to address foreign interference through advertising, including on online platforms like Google and Facebook.[253] It is instructive, however, that these measures all address the same mechanism of interference; a similar level of attention has not been paid to more long-standing and widespread mechanisms associated with traditional foreign interference.

279. It is essential that the government respond to the threat of foreign interference. To do so, the Committee believes that security and intelligence organizations should, at a minimum, have a common understanding of the threat, its magnitude and the various ways it manifests itself in Canada.

Interdepartmental coordination

280. Canada has been slow to react to the threat of foreign interference. A key turning point appears to have been the Russian interference in the 2016 U.S. presidential election, which clearly and publicly demonstrated potential vulnerabilities in democratic processes. Thereafter, the government established a number of interdepartmental fora to address electoral security and hostile state actors in late 2017 and 2018: heretofore, most of that activity has involved policy processes to define and understand the problem and the tools available to respond. Before that, government efforts to respond to discrete acts of foreign interference were conducted and coordinated on an ad hoc, case-by-case basis. The Committee reviewed three cases that occurred during the period under review. These cases revealed the strengths and weaknesses of Canada's current approach to addressing foreign interference.

281. Security and intelligence organizations have taken tangible measures to address instances of foreign interference. This is both a strength and a weakness: action is being taken, but usually against only one aspect of a state's foreign interference. In each of the cases reviewed by the Committee, individual organizations developed measures to address or counter a hostile state, engaged other members of the security and intelligence community, and implemented those measures, albeit with varying degrees of success. [*** The following sentence was revised to remove injurious or privileged information. It describes a government response to a state's foreign interference. ***] By contrast, the case of the government's response to China's Operation Fox Hunt *** focused on *** Chinese

---

[252] J. Michael Cole, "The Hard Edge of Soft Power: Understanding China's Influence Operations Abroad," *Macdonald-Laurier Institute*, October 2018.

[253] *Elections Modernization Act*, S.C. 2018, c. 31, https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2018_31/.

interference, *** to support criminal investigations of other states and to properly identify and remove persons ineligible to be in Canada. Similarly, the government's response to the Salisbury incident was in part based on Russian interference in Canada's democracy, but would only have occurred in the context of Russia's assassination attempt in the United Kingdom. In short, government responses were piecemeal, responding to specific instances of foreign interference but leaving unaddressed the many other areas where Canadian institutions and fundamental rights and freedoms continue to be undermined by hostile states.

282. The responsibilities of individual departments play a significant role in shaping government responses to foreign interference. That is to be expected: Canada's system of ministerial accountability gives individual ministers and departments significant autonomy over their respective mandates. The most important outcome is that individual organizations are generally responsible for determining when a threat should be addressed and the means to do so. As shown in the case studies – and to their credit – both CSIS and GAC have done so *** In each case, those organizations engaged others in the security and intelligence community prior to acting. However, this approach has limitations.

283. The most important limitation is inherent in the mandate and responsibilities of each organization. The Committee is concerned that having any one organization take the lead on determining if and how to respond to foreign interference will mean that considerations related to that organization's mandate will take precedence over other considerations. For example, GAC's mandate is to represent Canada's interests abroad. Among other things, it is responsible for managing diplomatic relations, addressing consular issues and promoting international trade. It also possesses and implements the majority of Canada's tools to respond to foreign interference, a threat that manifests itself in a domestic context.

284. In short, GAC is on the foreign policy end of a domestic security problem. Its leadership on determining if and how to respond to foreign interference means that foreign policy considerations, which are often clear and immediate (e.g., *** a state will not import a commodity from Canada), will take precedence over considerations of domestic harms, which are often vague and long term (e.g., *** a state's activities undermine free speech).

285. The Committee is also concerned that ad hoc coordination on specific instances of foreign interference is too narrow. Focusing on one issue risks not considering the broader challenges posed to ethnocultural groups and fundamental institutions. It also risks not considering all available tools and options. In that context, the Committee supports the government's recent analysis of the value of a broader approach to hostile state activity:

> Facilitating the participation of the full range of policy and operational capacity within and outside the federal system would support a more comprehensive analysis of an increasingly complex and ever-evolving threat, assessment of risks and

> opportunities of action, implications of inaction, the role of deterrence, and the levers and authorities available.[254]

Intergovernmental and public engagement

286. To advance their interests, foreign states target sub-national governments, specific ethnocultural communities and the public more generally. It is therefore essential that the government engage fundamental institutions and the public to raise their awareness of the threat posed by foreign interference and to start building a 'whole of Canada' defence. The importance of this engagement has been recognized for some time. In 1981, the McDonald Commission recommended:

> Ministers and Parliamentarians with responsibilities relating to security and intelligence should endeavour to provide the public with all information possible about the security of Canada, the threats to it and steps taken to counter those threats so that a more informed public opinion can address with some understanding the major issues relating to the work of a security intelligence agency.[255]

287. The government's engagement with sub-national levels of government has been inconsistent and uninformative. In 2017, the NSIA gave essentially the same high-level presentation to the clerks of the provinces and territories on national security threats, including foreign interference, on two separate occasions. The Committee believes this was a missed opportunity to increase formal engagement and coordination with sub-national levels of government. The presentations lacked the level of detail provided by the NSIA to Ontario provincial security advisors in a 2018 speech, which more fully explained the threats facing Canada's society and institutions. For its part, Public Safety Canada is essentially absent in this field.

288. Individual departments conduct outreach to sub-national counterparts. CSIS is particularly active in this respect, engaging provincial and municipal governments and individual police services. Its ability to share information is limited, however, by the absence of Secret-level clearances in most sub-national organizations. Moreover, CSIS efforts are conducted for the most part at the regional level and are not part of a strategic program of outreach. For its part, the RCMP has begun to engage local police forces on the threat posed by foreign interference. The RCMP's approach is hindered, however, because it does not make a distinction between espionage and foreign interference, ***[256] As a result, the Committee is concerned that foreign interference investigations will continue to be conducted on a one-off or ad hoc basis, in many cases by local police, and will not inform a broader understanding of the threat to national security, domestic sovereignty and the rights of Canadians.

---

[254] PCO, Countering Hostile State Activity: The Canadian Perspective, March 2018.
[255] McDonald Commission of Inquiry, *Part VIII A Plan for the Future: Direction and Review of the Security Intelligence System*, Government of Canada, 1981, http://publications.gc.ca/collections/collection_2014/bcp-pco/CP32-37-1981-2-2-2-eng.pdf.
[256] Working meeting between the NSICOP Secretariat and officials from CSIS, GAC, PCO, Public Safety Canada and the RCMP, April 26, 2019.

289. These limitations are reflected in the public's perception of the government's response. For example, in a spring 2019 presentation to the Standing Senate Committee on Foreign Affairs and International Trade, the Secretary General of Amnesty International Canada noted that those who are targeted do not know whether to turn to CSIS, the RCMP or municipal police, and that they rarely receive a coherent response from officials.[257]

290. The government's public engagement on foreign interference has also been limited. Public pronouncements by ministers have focused on efforts to ensure the integrity of the 2019 federal election, but not the broader threats and risks to Canadian society. There are no strategies or threat assessments to inform Canadians of foreign interference analogous to the yearly reports on terrorism. Similarly, there is almost no public engagement by senior levels of government. The exception is the Director of CSIS, who has engaged in an open and frank dialogue on the nature of the threat in a public setting. Through its academic outreach and unclassified publications, CSIS has also tried to increase public awareness and better inform government research and analysis. These activities are essential to strengthen public awareness of threats to Canada.

291. The Committee acknowledges the challenges in communicating information to fundamental institutions due to the sensitive nature of the information and the necessary independence of these institutions. However, these challenges should not impede government organizations from engaging Canadian institutions more thoroughly on the significant threats they face.

International cooperation

292. Canada's engagement with its allies and like-minded states to establish common principles to define and respond to the threat of foreign interference is in its early stages. Its efforts should continue for at least two reasons. First, Canada's approach supports the international rules-based order, particularly to clarify acceptable and unacceptable state behaviour. Second, it undermines efforts by hostile states to divide and isolate their targets by developing a common front. The PRC and the Russian Federation are *** perpetrators of foreign interference against Canada and its allies, and have proven particularly adept at using rewards and punishments to keep states in line with their interests. While Canada and its allies will always have different economic and political interests with these states, commonly agreed red lines and responses would serve to protect all. This is particularly important for Canada as a global middle power.

[257] Rachel Emmanuel, "China targeting human-rights activists in Canada, Senate committee told," *Globe and Mail*, June 6, 2019, https://www.theglobeandmail.com/politics/article-china-targeting-human-rights-activists-in-canada-senate-committee.

Conclusion

293. Foreign interference represents a significant threat to Canada's society and fundamental institutions. However, until the last several years it has mainly been considered the responsibility of security and intelligence organizations. Two states have done much to bring the threat into sharper relief: the Russian Federation, through its cyber efforts to undermine the U.S. presidential election and other democratic processes around the globe; and the PRC, through its broad-based strategy to covertly advance its interests in a number of countries, most publicly Australia and New Zealand. The Government of Canada is starting to address this issue, albeit under the broader ambit of 'hostile state activities.'

294. There is work to be done. This review shows that, for years, CSIS has investigated and reported on the threat posed by foreign interference by a number of states. It has assessed that Canada is an "attractive and permissive target."[258] The government's new focus is in its earliest stages and has yet to markedly change this environment. Engagement of sub-national levels of government remains cursory or limited by institutional challenges. Public engagement is almost non-existent, save for recent efforts by the Director of CSIS. Organizations within the security and intelligence community differ on how they define the problem and how they understand its gravity and prevalence. Reactions to foreign interference remain ad hoc and case-specific, rarely putting them in their broader context. The response is typically led by single organizations and the tools to counter are most often diplomatic. Understandably, this tends to result in foreign policy considerations being given greater weight than longer-term domestic risks, which are often harder to articulate as concrete harms. No organization represents the longer-term interests of Canadian sovereignty and fundamental values.

295. The government must do better. Canada's long-term security depends on the integrity of its sovereignty in decision-making, strong and independent fundamental institutions, and the protection of the rights and freedoms of Canadians. The government's approach must be based on a refined calculation of our collective interests and, most importantly, a continued emphasis on Canada's liberal democratic values. In that context, the Committee agrees with the following sentiment:

> Democratic values cannot be taken for granted. We must not become complacent in thinking that our own long-standing democracies are not susceptible to foreign interference. The openness of our societies is what make us vulnerable, but is a core component of democracy that contributes to our resilience and cannot be compromised.[259]

The threat is real, if often hidden. If it is not addressed in a comprehensive, whole-of-government approach, foreign interference will slowly erode the foundations of our fundamental institutions, including our system of democracy itself. The Committee expects that its review and recommendations will highlight important areas within which to work.

---

[258] CSIS, Foreign Espionage and Influenced Activities, Briefing material for DIR to Ambassador, undated.
[259] GAC, Reinforcing Democracy – Addressing Foreign Interference Issue Note, February 28, 2018.

Findings

296. The Committee makes the following findings:

F8. Some foreign states conduct sophisticated and pervasive foreign interference activities against Canada. Those activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. (Paragraphs 136–175)

F9. CSIS has consistently conducted investigations and provided advice to government on foreign interference. (Paragraphs 195–201)

F10. Throughout the period under review, the interdepartmental coordination and collaboration on foreign interference was case-specific and ad hoc. Canada's ability to address foreign interference is limited by the absence of a holistic approach to consider relevant risks, appropriate tools and possible implications of responses to state behaviours. (Paragraphs 219–227 and 280–285)

F11. Foreign interference has received historically less attention in Canada than other national security threats. This is beginning to change with the government's nascent focus on "hostile state activities." Nonetheless, the security and intelligence community's approach to addressing the threat is still marked by a number of conditions:

- There are significant differences in how individual security and intelligence organizations interpret the gravity and prevalence of the threat, and prioritize their resources. (Paragraphs 276–279)
- In determining the measures the government may use to address instances of foreign interference, responses address specific activities and not patterns of behaviour. Furthermore, the government's approach gives greater weight to short-term interests (e.g., foreign policy) than longer-term considerations (e.g., risks to freedoms, rights and sovereignty). (Paragraphs 281–285)

F12. Government engagement on foreign interference has been limited.

- With the exception of CSIS outreach activities, the government's interaction with sub-national levels of government and civil society on foreign interference is minimal. (Paragraphs 256–267)
- Engagement is limited in part by the lack of security-cleared individuals at the sub-national level. (Paragraph 261)
- There is no public foreign interference strategy or public report similar to those developed for terrorism or cyber security. (Paragraphs 289–291)

F13. Canada is working increasingly with its closest allies and partners to address foreign interference. This is essential for Canada. (Paragraphs 268–274)

Recommendations

297. The Committee makes the following recommendations:

R5. The Government of Canada develop a comprehensive strategy to counter foreign interference and build institutional and public resiliency. Drawing from the Committee's review and findings, such a strategy should:

a. identify the short- and long-term risks and harms to Canadian institutions and rights and freedoms posed by the threat of foreign interference;

b. examine and address the full range of institutional vulnerabilities targeted by hostile foreign states, including areas expressly omitted in the Committee's review;

c. assess the adequacy of existing legislation that deals with foreign interference, such as the *Security of Information Act* or the *Canadian Security Intelligence Service Act,* and make proposals for changes if required;

d. develop practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states;

e. establish regular mechanisms to work with sub-national levels of government and law enforcement organizations, including to provide necessary security clearances;

f. include an approach for ministers and senior officials to engage with fundamental institutions and the public; and

g. guide cooperation with allies on foreign interference.

R6. The Government of Canada support this comprehensive strategy through sustained central leadership and coordination. As an example of a centralized coordinating entity to address foreign interference, the Committee refers to the appointment and mandate of the Australian National Counter Foreign Interference Coordinator.

298. The Committee reiterates its recommendation from its *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*:

In the interest of national security, members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada. In addition, Cabinet Ministers should be reminded of the expectations described in the Government's *Open and Accountable Government*, including that Ministers exercise discretion with whom they meet or associate, and clearly distinguish between official and private media messaging, and be reminded that, consistent with the *Conflict of Interest Act*, public office holders must always place the public interest before private interests.

Chapter 3: The Canada Border Services Agency's National Security and Intelligence Activities

Introduction

299. This chapter examines the national security and intelligence activities of the Canada Border Services Agency (CBSA) in support of its mandate.

300. CBSA was established in December 2003 by an Order in Council that amalgamated the border and enforcement personnel of Citizenship and Immigration Canada (now Immigration, Refugees and Citizenship Canada or IRCC) with the customs control aspects of the Canada Customs and Revenue Agency (now the Canada Revenue Agency) and the Canadian Food Inspection Agency.[1] CBSA was formalized in statute in the *Canada Border Services Agency Act* (the CBSA Act), which received Royal Assent in November 2005.

301. The CBSA Act mandates CBSA to "[provide] integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation."[2]

302. CBSA has a planned budget of $1.87 billion for 2019–2020.[3] It has a staff of approximately 14,000 employees, including over 6,400 uniformed officers who provide services at approximately 1,200 points across Canada and at 39 international locations. CBSA manages 117 land-border crossings and operates customs-controlled areas at 15 of Canada's major international airports. It also carries out marine operations at major ports, performs operations at 27 rail sites and examines international mail at three mail processing centres.[4]

303. CBSA's role in ensuring the security of Canada rests primarily on its decisions concerning the admissibility of people and goods into Canada. These decisions are made across multiple modes of travel, including air, rail, marine and land (or highway). In the area of national security, inadmissibility decisions are essential in countering threats such as terrorism, espionage, foreign interference and proliferation. It should be emphasized, however, that inadmissibility is far more often invoked for reasons unrelated to national security.

---

[1] Order in Council P.C. 2003-2063 of December 12, 2003, registered as SI/2003-215; Order in Council P.C. 2003-2064 of December 12, 2003, registered as SI/2003-216; and Order in Council P.C. 2003-2065 of December 12, 2003, registered as SI/2003-217.

[2] *Canada Border Services Agency Act*, s. 5(1).

[3] Canada Border Services Agency (CBSA), *Canada Border Services Agency 2019–20 Departmental Plan*, 2019. www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/rpp/2019-2020/report-rapport-eng.pdf.

[4] CBSA, "About the CBSA, What We Do," www.cbsa-asfc.gc.ca/agency-agence/what-quoi-eng.html.

304. CBSA uses intelligence to support its mandate to administer and enforce Canada's immigration and customs legislation. Specifically, intelligence is used to develop a risk management strategy to identify border-related threats as far in advance as possible before they arrive at a Canadian port of entry. Intelligence is also used to interdict these threats and to mitigate them.[5] Collectively, this is known as "pushing the border out."[6] CBSA does not have a stand-alone intelligence mandate. CBSA's intelligence activities primarily support its own enforcement responsibilities.

305. In general, therefore, CBSA is best understood as an organization whose primary mandate is based on making admissibility decisions concerning goods and people and facilitating the flow of legitimate trade and travel: its national security responsibilities flow from that mandate. CBSA has a small program that conducts limited intelligence activities to support operations across its full mandate. As the President of CBSA stated during an appearance, CBSA plays a "niche" role in the areas of national security and intelligence.[7]

Review methodology

306. On September 27, 2018, the Committee decided to undertake a review of CBSA's national security and intelligence activities. On November 8, 2018, the Chair of the Committee provided a notification letter to the Minister of Public Safety and Emergency Preparedness. On April 26, 2019, the Chair provided a notification letter to the Minister of Immigration, Refugees and Citizenship.

307. The Committee identified three main objectives for its review of CBSA's national security and intelligence activities. First, it sought to determine the role of CBSA within the national security and intelligence community. Second, it sought to determine the national security and intelligence activities of CBSA, and delineate those from CBSA's overall range of operations. Third, it aimed to determine the authorities under which CBSA conducts national security and intelligence activities.

308. Notwithstanding CBSA's broad mandate, the Committee focused its review on three key areas most closely aligned with CBSA's national security and intelligence activities:[8]

- CBSA's governance over national security and intelligence activities in CBSA's Enforcement and Intelligence Program, including ministerial direction provided to CBSA.
- CBSA's conduct of sensitive national security and intelligence activities, specifically targeting, the use of confidential human sources, covert surveillance, lookouts, and CBSA's participation in joint force operations; and

---

[5] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.
[6] See: CBSA, "Access to Information and Privacy. Information about Programs and Information Holdings 2018 (formerly Info Source)", www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html.
[7] CBSA, Remarks of the CBSA President and Vice-President, NSICOP hearing, May 7, 2019.
[8] CBSA has a broad mandate for border security, immigration screening, the admissibility of people and goods, the collection of revenue from import taxes, and administering trade legislation and trade agreements. CBSA, "About the CBSA, What We Do," www.cbsa-asfc.gc.ca/agency-agence/what-quoi-eng.html.

- CBSA's relations with its key partners in the areas of national security and intelligence: IRCC, the Royal Canadian Mounted Police (RCMP) and the Canadian Security intelligence Service (CSIS).

309. The Committee did not examine CBSA activities outside of these areas, including calls by civil society groups for independent review of officer conduct.[9]

310. The Committee received more than 650 documents (approximately 16,000 pages) from CBSA in response to the terms of reference. These documents related to:

- national security and intelligence activities, departmental organization, and priorities;
- national security and intelligence resource expenditures;
- policies, operational bulletins and standard operating procedures;
- legal opinions;
- memoranda of understanding and agreements with other government departments, members of the national security and intelligence community, and international partners;
- ministerial directions;
- internal performance measurement and internal annual reports; and
- internal or external evaluations and audits of CBSA's activities.

311. CBSA officials briefed the Committee on the agency's national security and intelligence activities, internal and inter-departmental governance structures for national security and intelligence activities, and key relationships with IRCC, CSIS and the RCMP. CBSA officials also briefed the Committee on the operations of the National Border Operations Centre, the National Targeting Centre, the immigration security screening process and the National Security Screening Division, as well as on CBSA's role in implementing the government's intelligence priorities. As part of this review, CBSA provided detailed information on a case where immigration security screening failures resulted in an individual of national security concern being granted permanent residency in Canada.

312. This chapter begins by detailing the rationale behind the Committee's decision to conduct a review of CBSA's national security and intelligence activities, including the risks associated with such activities and the overall complexity of the CBSA mandate for border enforcement and administration. It then focuses more specifically on CBSA's role in national security and intelligence by describing past reviews in these areas, CBSA authorities to conduct national security and intelligence activities, and key partnerships. It then examines specific CBSA national security and intelligence activities and the internal system of governance CBSA has in place for their control. The Committee provides its assessment and finishes with its findings and recommendations.

---

[9] See for example, Canadian Council for Refugees, "Proposed CCR model for a CBSA Accountability Mechanism," https://ccrweb.ca/sites/ccrweb.ca/files/ccr-cbsa-accountability-model.pdf.

Background and rationale for review

313. The Committee's decision to conduct a review of CBSA's national security and intelligence activities was based on a number of considerations. The first is that the scale, scope and nature of national security and intelligence activities conducted by CBSA is not widely known, nor well understood. As noted by a former President of CBSA, "there's a need to bring greater public confidence in terms of the activities of CBSA."[10]

314. The second consideration is that CBSA's activities have not been subject to regular, independent, external review. Civil society experts, academics, and members of the judicial and legislative branches of government have expressed the need for CBSA's activities – including those pertaining to national security and intelligence – to be subject to independent review, and by extension, public criticism.[11] Although CBSA's full complement of national security and intelligence activities have never been reviewed by an independent, external review body, the Committee acknowledges that some areas have been examined by independent bodies (e.g., the 2017 review of scenario-based targeting for national security purposes by the Office of the Privacy Commissioner). The scope of previous external review of CBSA activities is discussed in paragraph 317.

315. The third consideration is the overall complexity of the CBSA mandate, which includes administering over 90 acts of Parliament, regulations and international agreements. This complexity manifests in three ways. First, CBSA has concurrent roles of upholding Canada's security, supporting Canadian prosperity and serving the public (including as the government's second-largest revenue collector).[12] Second, CBSA officers must balance customs, intelligence, interdiction, enforcement, immigration and import inspection functions in the provision of integrated border services. Third, CBSA officers are responsible for the organization's intelligence and enforcement priorities while also enforcing numerous other acts and regulations in areas such as health or agriculture.[13]

---

[10] House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 1st Session, 42nd Parliament, November 22, 2016 (Luc Portelance testified as an individual).

[11] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities*, Ottawa, 2006; Standing Senate committee on National Security and Defence, *Vigilance, Accountability and Security at Canada's Borders*, June 2015; Standing Committee on Public Safety and National Security, *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*, May 2017; and Mel Cappe, Mind the Gap!, prepared for Public Safety and Emergency Preparedness Canada, June 19, 2017.

[12] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019; CBSA, "Supplementary Information Tables," *Departmental Plan 2018–19*, www.cbsa-asfc.gc.ca/ageny-agence/reports-rapports/rpp/2018-19/subprog-sousprog-eng.html.

[13] CBSA, Integrated Enforcement and Intelligence Priorities 2017/18-2019/20, undated.

316. The Committee's fourth consideration is the risks inherent in CBSA's national security and intelligence activities. These include:

- **Risks to an individual's rights under the *Canadian Charter of Rights and Freedoms*:** CBSA activities present risks to an individual's Charter rights. At the border, there is a reduced expectation of privacy and CBSA border services officers have the authority to search goods, conveyances and persons without a defined threshold.[14] Inside Canada, CBSA may affect Canadians' Charter rights through the conduct of sensitive intelligence activities, such as surveillance, scenario-based targeting and confidential human sources;[15]
- **Risks related to balancing the interdiction of high-risk travellers and the facilitation of legitimate travel and trade:** Risks may arise if CBSA casts its net too wide and focuses excess resources on low-risk goods and persons. Alternatively, risks may arise if CBSA focuses its efforts too narrowly and allows high-risk goods and persons to slip through the cracks;
- **Risks to Canada's international relations and reputation:** Engaging in sensitive activities, such as covert surveillance or the use of confidential human sources, may negatively affect Canadian relations with other countries or international organizations.[16] Granting admissibility to individuals of national security concern may cause allied nations to question Canada's ability to secure its borders; denying entry to legitimate travellers may cause bilateral irritants.[17]

---

[14] As noted by the Supreme Court of Canada, "People do not expect to be able to cross international borders free from scrutiny. It is commonly accepted that sovereign states have the right to control both who and what enters their boundaries." *R. v. Simmons*, [1988] 2 S.C.R. 495 at 49; *Customs Act*, 1985, s. 99.

[15] CBSA policies acknowledge this risk and are explicit that sensitive operational activities "cannot be conducted or continue if they infringe upon the lawful rights of others, most particularly including rights and freedoms set out in the *Charter*." As noted in the CBSA, *Standard Operating Procedures in support of the Confidential Human Source Policy.*

[16] CBSA, *Standard Operating Procedures in support of the Confidential Human Source Policy. Annex 1. CBSA – CHS Risk Assessment – Conceptual Framework*, undated.

[17] CBSA policies and standard operating procedures, such as those pertaining to the use of confidential human sources, outline these risks in detail, noting that these activities can bring "significant risks to the Agency [and can be] particularly intrusive." CBSA, *Standard Operating Procedures in support of the Confidential Human Source Policy*, undated.

Reviews, audits and evaluations of CBSA national security and intelligence activities

External review

317. The following external audits or reviews relate to specific aspects of CBSA's national security and intelligence activities:

- **Office of the Auditor General of Canada, Chapter 5: Keeping the Border Open and Secure – Canada Border Services Agency (2007):** This audit examined how CBSA identifies and interdicts high-risk people and goods, while facilitating the flow of those deemed low risk. It noted that CBSA does not have consistent recording or monitoring in place for its lookout system or for secondary examinations.
- **Office of the Auditor General of Canada, Chapter 5: Preventing Illegal Entry Into Canada (2013):** This audit examined the performance of selected CBSA and RCMP systems and practices in preventing the illegal entry of people into Canada. It found systems and practices for collecting, monitoring and assessing information regarding admissibility often do not work as intended, resulting in the illegal entry of high-risk individuals.
- **The House of Commons Standing Committee on Citizenship and Immigration: Standing on Guard for Thee: Ensuring Canada's Immigration System Is Secure (2013):** This study analyzed the security of Canada's immigration system. It recommended that CBSA be given authority to conduct exit checks and allocate more resources toward removing failed refugee claimants. It also recommended that CBSA and its federal partners improve information sharing and that Citizenship and Immigration Canada (CIC, now IRCC) and CBSA develop the capacity to collect intelligence outside of Canada.
- **The Standing Senate Committee on National Security and Defence: Vigilance, Accountability and Security at Canada's Borders (2015):** This study focused on how CBSA identifies and denies admissibility to persons and removes inadmissible persons who have entered Canada. It recommended the establishment of bodies both for oversight and for independent, civilian review and handling complaints for all CBSA activities. It recommended that the government implement an entry-exit system; ensure that CIC (now IRCC), CBSA, CSIS and the RCMP use all of their databases when screening foreign nationals; enhance CBSA's regional intelligence capabilities and information sharing with front-line officers; and ensure that CBSA officers are provided with the most up-to-date information concerning travellers.
- **The Office of the Privacy Commissioner: Canada Border Services Agency – Scenario-Based Targeting of Travellers – National Security (2017):** This audit analyzed the privacy implications of the national security scenarios within CBSA's scenario-based targeting program. It found that there is a risk that information disclosed by CBSA for the purpose of database checks may be retained and shared by federal partners and U.S. Customs and Border Protection. It also noted that CBSA measures the effectiveness of its national security scenarios against broad outcomes, making it difficult to accurately describe the efficacy of scenario-based targeting for identifying national security threats.

318. Several of CBSA's other activity areas are subject to external review or adjudication. For example, the Canadian International Trade Tribunal hears appeals of commercial disputes involving CBSA under the *Customs Act*. Additionally, the Immigration and Refugee Board conducts reviews of detentions made for immigration purposes, and holds admissibility hearings. The Office of the Auditor General audits CBSA's handling of public funds, and the Office of the Privacy Commissioner reviews CBSA's handling of personal information under the *Privacy Act*.

Internal audit and evaluation

319. Since 2011, CBSA has publicly released 86 internal audit and evaluation reports spanning the entire range of its operations.[18] CBSA provided the Committee with classified versions of selected reports, in response to the Committee's terms of reference. The following reports are particularly relevant to CBSA's national security and intelligence activities:

- **Evaluation of CBSA Participation in Joint Force Operations (2012):** This study evaluated the relevance and performance of CBSA participation in joint force operations. It found that CBSA objectives, goals and guidelines for participation in joint force operations are not clearly articulated. Additionally, it found that joint force operations have limited involvement from CBSA's National Headquarters and that the roles and responsibilities of personnel within different CBSA programs were unclear, which negatively affected relationships with external partners. To clarify CBSA's roles and responsibilities, the study recommended that CBSA update its joint force operation policy and the mandates of respective branches within CBSA. CBSA agreed with all recommendations.[19]
- **Evaluation of the Intelligence Program (2014):** This evaluation assessed the relevance and performance of CBSA's Intelligence Program. It found that there is continued need for CBSA's Intelligence Program and that senior managers required additional guidance on how to allocate resources in accordance with CBSA's enforcement and intelligence priorities. The evaluation also found that the roles and responsibilities of the Intelligence Program are generally not understood within CBSA. The report recommended that CBSA increase the transparency of its intelligence function internally, clarify how the Intelligence Program will support integrated enforcement activities, and provide internal guidance on how progress against priorities will be assessed. CBSA agreed to all recommendations.[20]
- **Audit of Immigration Enforcement (2016):** This audit analyzed CBSA's Inland Enforcement Program. It found that CBSA's governance structure for inland enforcement could be improved to more effectively escalate and resolve program risks and issues. The audit recommended that CBSA more clearly describe the role of each governance body within its broader governance

---

[18] CBSA, "Audit and Evaluation Reports," www.cbsa-asfc.gc.ca/reports-rapports/ae-ve/menu-eng.html.

[19] CBSA, Internal Audit and Program Evaluation Directorate, Program Evaluation Division, *CBSA Participation in Joint Force Operations: Evaluation Study*, February 9, 2012. www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2012/jfo-opc_fn-eng.html.

[20] CBSA, Internal Audit and Program Evaluation Directorate, Program Evaluation Division, *Evaluation of the Intelligence Program*, April 2014.

architecture and improve the quality of information provided to these decision-making bodies. CBSA agreed to all recommendations.[21]

- **Audit of Operation Syrian Refugee – CBSA Security Screening (2017):** This audit analyzed the efficacy of CBSA's national security screening program as part of Operation Syrian Refugee, the multi-departmental, multi-stakeholder response to the government's relocation of Syrian refugees from 2015–2016. It found that gaps were present in the security screening process due to systems and human errors. It also found inconsistencies between IRCC's and CBSA's records and systems with respect to national security screening of refugee applicants. The audit recommended that CBSA automate controls within its case management system to reduce errors and implement a revised quality assurance program. CBSA agreed with both recommendations.[22]

320. CBSA conducted two substantive studies of its Targeting Program, in 2015 and 2016.[23] The studies found that the Targeting Program has continued relevance, but that gaps existed within CBSA's governance and performance measurement structures. The studies recommended that CBSA finalize and approve performance measurement tools to better inform program decision-making; strengthen oversight and clarify key roles and responsibilities; and formalize a risk management process for the Targeting Program. CBSA agreed with all recommendations.

321. Other departments and agencies have assessed various elements of CBSA operations as part of their horizontal evaluations. For example, IRCC reviewed CBSA's ability to remove failed refugee claimants as part of its 2016 Evaluation of the In-Canada Asylum System Reforms.[24] In another 2016 evaluation, Public Safety Canada assessed the management of cases where classified information was used to make inadmissibility decisions, and where non-citizens were alleged or determined to be inadmissible on security grounds, or were released with conditions, based on that information. The study included an assessment of the combined activities of nine federal departments and agencies, including CBSA.[25]

---

[21] CBSA, Internal Audit and Program Evaluation Directorate, *Audit of Immigration Enforcement*, December 2016, www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2016/ie-emi-eng.html.

[22] CBSA, Internal Audit and Program Evaluation Directorate, *Audit of Operation Syrian Refugee – CBSA Security Screening (draft)*, April 2017.

[23] CBSA, *Audit of National Targeting*, December 2015, www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2015/nt-cn-eng.html; CBSA, Internal Audit and Program Evaluation Directorate, *Evaluation of the Canada Border Services Agency Targeting Program*, January 2016, www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2016/tp-pc-eng.html; Note: the Committee also received classified versions of these audits.

[24] Immigration, Refugees and Citizenship Canada (IRCC), Evaluation Division, *Evaluation of the In-Canada Asylum System Reforms*, April 2016. www.canada.ca/en/immigration-refugees-citizenship/corporate/reports-statistics/evaluations/canada-asylum-system-reforms.html.

[25] Public Safety Canada, *2014–2015 Horizontal Evaluation of the Immigration and Refugee Protection Act Division 9/National Security Inadmissibility Initiative*, June 28, 2016. www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-irpa/index-en.aspx.

New and proposed review

322. In addition to the Committee, the newly formed National Security and Intelligence Review Agency (NSIRA) may review CBSA's national security and intelligence activities. The *National Security and Intelligence Review Agency Act*, which establishes the review body, became law on June 21, 2019, when Bill C-59, An Act respecting national security matters, received Royal Assent. NSIRA may review all national security and intelligence activities conducted by government agencies and departments.[26] While NSIRA would not be statutorily obligated to regularly review CBSA's national security or intelligence activities, it may choose to review CBSA as the subject of its special or annual reports.

323. On May 7, 2019, the Minister of Public Safety and Emergency Preparedness introduced Bill C-98, An Act to amend the Royal Canadian Mounted Police Act and the Canada Border Services Agency Act and to make consequential amendments to other Acts. This legislation would expand the mandate of the Civilian Review and Complaints Commission (CRCC) to include the independent review of any activity (outside of national security) conducted by CBSA and the investigation of public complaints concerning CBSA officer conduct. To reflect these changes, the CRCC would be renamed the Public Complaints and Review Commission. At the time of drafting this annual report, the bill had been referred to the Senate for first reading.

---

[26] *National Security and Intelligence Review Agency Act,* Part 1, Section 8(1) at www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent#ID0EAIAG.

Authority structure for national security and intelligence activities

324. CBSA administers and enforces over 90 acts, regulations and international agreements on behalf of other federal departments and agencies, the provinces, and the territories.[27] This collection of acts and regulations is known as CBSA's program legislation. The CBSA Act, the *Customs Act*, and the *Immigration and Refugee Protection Act* (IRPA) are the most relevant for examining CBSA's national security and intelligence activities. To fulfill its obligations under its program legislation, CBSA uses several operational programs and activities, including five areas of greater sensitivity: targeting, covert surveillance, the use of confidential human sources, lookouts, and CBSA's participation in joint force operations. Each of these activity areas will be discussed below.

325. CBSA has no explicit statutory authority for conducting these sensitive national security and intelligence activities. Rather, CBSA's authority for undertaking those activities stems from its mandate to enforce its program legislation. This is consistent with the principles of the *Interpretation Act*. Put simply, if CBSA is to administer and enforce its program legislation, it must be able to investigate suspected contraventions of that legislation. Moreover, CBSA's authority to conduct certain activities, such as covert surveillance or the use of confidential human sources, is also rooted in policing and common law powers, which are supported by significant jurisprudence (see paragraphs 331 and 332). In any event, CBSA activities must have a direct link to its mandate and program legislation.[28]

The *Canada Border Services Agency Act*

326. The CBSA Act establishes CBSA and its mandate. Importantly, the Act does not list any national security, intelligence or law enforcement activities that CBSA officers are authorized to conduct. The Act provides CBSA with a mandate to provide integrated border services that:

- support national security and public safety priorities; and
- facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation.[29]

The Act authorizes CBSA to support the administration and enforcement of its program legislation, including the *Customs Act* and IRPA.[30]

---

[27] A list of these acts, regulations and agreements can be found at www.cbsa-asfc.gc.ca/agency-agence/actreg-loireg/legislation-eng.html#_s1.

[28] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019. See also, CBSA, Review of CBSA national security and intelligence activities, Presentation to NSICOP, May 7, 2019.

[29] *Canada Border Services Agency Act*, s. 5(1).

[30] *Canada Border Services Agency Act,* 2005, ss. 2(*a*) – 2(*d*), and 5(1)(*a*).

The *Customs Act*

327. Along with IRPA, the *Customs Act* is the primary piece of legislation administered and enforced by CBSA. The *Customs Act* sets out the legislative authority to control the importation and exportation of goods, and allows CBSA officers to examine, detain or seize goods in cases of non-compliance. The *Customs Act* provides CBSA authority to question and search persons coming in or out of Canada, search individuals and conveyances, detain individuals, and oblige travel service providers to provide Advance Passenger Information data on each air passenger before their arrival to Canada.[31]

The *Immigration and Refugee Protection Act*

328. Responsibilities for the administration and enforcement of IRPA is shared by the Ministers of Public Safety and Emergency Preparedness and Immigration, Refugees and Citizenship with specific responsibilities being given to the Ministers of Employment and Social Development Canada and Justice. IRPA provides designated CBSA officers with the authority to make admissibility decisions for persons seeking entry to Canada and to board and inspect any means of transportation arriving in Canada.[32]

329. CBSA is responsible for admissibility determinations pursuant to the authority under IRPA of the Minister of Public Safety and Emergency Preparedness.[33] With respect to national security, for example, a person may be found inadmissible for reasons of:

- **security**, by engaging in, or being part of a group that engages in, espionage, subversion or terrorism; being a danger to the security of Canada; or engaging in acts of violence that would or might endanger the lives or safety of persons in Canada;[34]
- **human or international rights violations**, by committing a war crime, genocide or crime against humanity outside of Canada; being a senior official in the service of a government that the Minister believes has engaged in terrorism, systemic or gross human rights violations, genocide, a war crime or a crime against humanity;[35] or
- **organized criminality**, by being a member of an organization that is believed on reasonable grounds to have engaged in organized criminality, or furthering the commission of an offence

---

[31] The *Customs Act*, 1985, ss. 99(1), 101, 110(1), 11, 98(1), 99(1)(f), 163.5(1)(2)(3) and 107.1. Advance Passenger Information consists of an individual's full name, date of birth, citizenship or nationality, gender, travel document number, and reservation record locator or file number. A "conveyance" is understood as a "means of transporting or carrying. A conveyance will include a vehicle such as a bus, ship, airplane, truck, train or automobile." See www.canada.ca/en/revenue-agency/services/forms-publications/publications/p-067r/a-conveyance-cargo-container.html.

[32] *Immigration and Refugee Protection Act* (IRPA), 2001, ss. 18(1), 15(3), 18(2) and 139.

[33] Admissibility determinations can involve CBSA and the Immigration and Refugee Board, to whom the Minister of Public Safety and Emergency Preparedness can refer, via CBSA, cases for foreign nationals or permanent residents who are believed to have contravened IRPA. For more information, see https://irb-cisr.gc.ca/en/legal-policy/procedures/Pages/ProcessAdmEng.aspx, and www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/ae-ve/2018/imp-pa-eng.html.

[34] IRPA, 2001, ss. 34(1).

[35] IRPA, 2001, s. 35(1). Under this section, a determination of inadmissibility may also be made in reference to an individual being the subject of sanctions, as listed in ss. 35(1)(*c*), 35(1)(*d*), and 35(1)(*e*).

outside Canada that, if committed in Canada, would constitute such an offence, or engaging in activity such as people smuggling, trafficking in persons, or money laundering or other proceeds of crime.[36]

330. IRPA also authorizes CBSA officers to issue a warrant for the arrest and detention of a permanent resident or a foreign national who the officer has reasonable grounds to believe is inadmissible and is a danger to the public or a flight risk. However, an officer does not require a warrant in all cases. Specifically, an officer may detain or arrest a foreign national on entry if the officer is not satisfied with the identity of the foreign national, considers it necessary to complete an examination, or has reasonable grounds to suspect that the individual is inadmissible for reasons of security, violation of human or international rights, or serious or organized criminality.[37]

The *Interpretation Act*

331. CBSA stated that the *Interpretation Act* is the key enabling authority for the conduct of its national security and intelligence activities.[38] The *Interpretation Act* states that, "[w]here power is given to a person, officer, or functionary to do or enforce the doing of any act or thing, all such powers as are necessary to enable the person, officer or functionary to do or enforce the doing of the act or thing are deemed to be also given."[39] For CBSA, this means that where the CBSA Act provides CBSA the power to administer and enforce its program legislation, the *Interpretation Act* gives CBSA the authority to perform other activities, such as scenario-based targeting, that support the execution of its mandate.

332. [*** This paragraph was revised to remove injurious or privileged information. The paragraph notes that CBSA officers have a duty to enforce specific statutes, and must, by implication, have the necessary tools to identify transgressions of those laws. As stated by the Federal Court in 1992, this authority rests on "an established principle of common law [codified in subsection 31(2) of the *Interpretation Act*], that '[t]he powers conferred by an enabling statute include not only such as are expressly granted but also, by implication, all powers which are reasonably necessary for the accomplishment of the object intended to be secured.'"[40] ***]

---

[36] IRPA, 2001 s. 37(1).

[37] For more information on CBSA powers for arrests, detentions and removals see: www.cbsa-asfc.gc.ca/security-securite/arr-det-eng.html. See also IRPA, 2001, ss. 34(1), 15(1), 37(1), 55(1), 55(2)(*a*) and 55(2)(*b*).

[38] CBSA, Review of CBSA National Security and Intelligence Activities: Joint Hearing with the Canada Border Services Agency, Canadian Security Intelligence Service (CSIS), and Royal Canadian Mounted Police (RCMP), Presentation to NSICOP, May 16, 2019.

[39] *Interpretation Act*, s. 31(2), regarding Ancillary Powers.

[40] *Her Majesty the Queen v. Brode* and *Chrysler Canada Ltd. v. Canada (Competition Tribunal)*, [1992] 2 S.C.R. 394, (at p. 410) https://www.canlii.org/en/ca/scc/doc/1992/1992canlii68/1992canlii68.html. Judge Gonthier quotes *Halsbury's Laws of England*, vol. 44, 4th ed., para. 934, p. 586.

Other acts

333. CBSA also administers and enforces a number of other acts, regulations and agreements that have a national security or intelligence component. These include the following:

- ***Proceeds of Crime (Money Laundering) and Terrorist Financing Act*:** From a national security perspective, CBSA's reporting on cross-border movements of currency or monetary instruments, forfeitures, or seizures contributes to the ability of the Financial Transactions and Reports Analysis Centre (FINTRAC) to detect, prevent and deter the financing of terrorist activities.
- **Import and Export Control Legislation:** The *Export and Import Permits Act,* the *Customs Act*, the *Nuclear Safety and Control Act*, and the *Special Economic Measures Act* frame CBSA's role in Canada's efforts to counter the proliferation of controlled dual-use goods and weapons of mass destruction.
- **The *United Nations Act*:** Where the United Nations (through the Security Council) adopts measures (e.g., sanctions) such as complete or partial interruption of economic relations and of rail, sea, air, postal or other means of communication, CBSA works with the RCMP to enforce regulations brought into force pursuant to the *United Nations Act*.[41]

[41] For more information, see www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/legislation-lois.aspx?lang=eng.

National security and intelligence partners

334. CBSA is a core part of Canada's security and intelligence community because management of the border is a core security issue for Canada.[42] CBSA's role in that community is to support national security and public safety priorities by determining the admissibility of persons or goods to Canada on security grounds and by addressing contraventions of border legislation. CBSA has stated that in the execution of its mandate, several of its programs may have national security "outcomes," that is, direct or indirect national security benefits that are a consequence of CBSA's work to identify and interdict high-risk people or goods before they enter Canada.[43] CBSA works with both Canadian and international partners.

335. CBSA maintains key partnerships in the security and intelligence community. Its core relationships are with IRCC, the RCMP and CSIS. These relationships involve the majority of CBSA's national security and intelligence activities, including those of higher risk or sensitivity. Pursuant to various sections of the CBSA Act, CBSA enters into agreements with other departments or agencies and international partners in the fulfillment of its mandate.[44] The agreements are formalized through official memoranda of understanding between the organizations, which describe roles and responsibilities, authorities for operational cooperation, administrative procedures for dispute resolution, and parameters and authorities for information sharing.

336. Information sharing is key to CBSA's relationships. CBSA's authority to share national security-related information stems from four main elements: the *Customs Act*; IRPA and its regulations; the *Security of Canada Information Disclosure Act* (SCIDA); and the *Privacy Act*.[45] The specific types of information that CBSA may share, pursuant to these acts, are listed in Table 13.

---

[42] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.

[43] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.

[44] CBSA Act, ss. 5(1)(*d*), 5(2) and 13(2)(*b*).

[45] During the period under review, the *Security of Canada Information Sharing Act* (SCISA) was renamed the *Security of Canada Information Disclosure Act* (SCIDA).

Statute	Type of Information	Sharing in Practice
Customs Act, s. 107	Customs information	This includes information of any kind that relates to the enforcement and administration of the *Customs Act*, including information about commercial shipments or conveyances, Advance Passenger Information, importation and exportation information, and customs infractions. It may also include any other information gathered in the context of CBSA's routine customs examinations, including officer questions and passenger responses as part of a customs examination.
IRPA, s.150.1(1)(*b*), and associated *Immigration and Refugee Protection regulations*)[46]	Immigration information	This authorizes the making of regulations to permit information sharing, including any information collected, pursuant to IRPA, which may be shared for the purposes of national security, the defence of Canada or the conduct of international affairs.
Security of Canada Information Disclosure Act, s. 5(1)	Information that is relevant to 16 other agencies and departments' responsibilities in respect of activities that undermine the security of Canada	This includes relevant information concerning interference with the capability of the Government of Canada; espionage, sabotage or foreign-influenced activities; terrorism; and the proliferation of nuclear, chemical, radiological or biological weapons. This Act applies to sharing with other government departments.
Privacy Act, s. 8	Personal information	This may include an individual's name, contact information, biographical information, date and place of birth, criminal history, identity documentation, signature, traveller history, and immigration enforcement. It may also include information pertaining to an individual's biometric data, credit, education and finances. Pursuant to the *Privacy Act*, this information may be disclosed solely for the purpose for which it was obtained or for a use consistent with that purpose (see paragraph 337).[47] This means that information may only be collected if it is related to CBSA's program legislation, and shared under Section 8(2) of the *Privacy Act*.

Source: *Security of Canada Information Disclosure Act, S.C. 2015, c. 20, s. 2; Privacy Act. R.S.C., 1985, c. P-21. S.3.; and* www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html.

Table 13: CBSA's Information Sharing in Practice

[46] *Immigration and Refugee Protection Regulations* (Part 19.1, ss. 315.21, ss. 315.28, ss. 315.36) at https://laws-lois.justice.gc.ca/eng/regulations/sor-2002-227/page-8.html#docCont.

[47] This information may be disclosed only on the consent of the individual, or for any of the reasons set out in ss. 8(2)(*a*) to 8(2)(*m*) of the *Privacy Act*.

337. The *Privacy Act* includes a number of safeguards that limit the sharing of personal information. As noted in Table 13, information may be disclosed for the purpose for which it was obtained or for a use consistent with that purpose. The Treasury Board Policy on Privacy Protection defines "consistent use" as "a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled." Moreover, "[t]his means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out."[48] The *Privacy Act* also requires the designated minister to publish a personal information index at least once per year. This index must contain descriptions of all personal information banks, the purpose for which the personal information was obtained or compiled, a statement of consistent uses for which information may be disclosed, and a statement on the retention and disposal standards applied to information in the bank.[49]

338. CBSA collects information specific to the purposes of administering and enforcing its program legislation. Regarding CBSA support of national security and public safety priorities, Table 14 illustrates types and purposes for sharing collected information, authorities for disclosure, and policies to guide employee conduct and to mitigate risks in the sharing of information. In all areas, CBSA may share information with its domestic and international partners, pursuant to its specific purpose and authority regime for disclosure.

---

[48] Treasury Board Secretariat, *Policy on Privacy Protection,* www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510.

[49] *Privacy Act*. R.S.C., 1985m c, P-21, s. 11(1). For additional information on personal information banks and the consistent use of personal information in the context of CBSA activities, see: CBSA, "Access to Information and Privacy. Information about Programs and Information Holdings 2018 (formerly Info Sourcewww.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html.

Type of Information and Purpose for Sharing	Authority for Disclosure	CBSA Policy Guidance
Information regarding national security screening	*Privacy Act* (s. 8)	Policy on the Disclosure of Personal Information: s. 8 of the *Privacy Act*
IRPA information relevant to a threat to the security of Canada	*Privacy Act* (s, 8) and *Security of Canada Information Disclosure Act* (SCIDA) (s. 5(1))	Policy on the Disclosure of Personal Information: s. 8 of the *Privacy Act*
Customs information relevant to a threat to the security of Canada	*Customs Act* (s. 107) and SCIDA (s. 5(1))	Policy on the Disclosure of Customs Information: s. 107 of the *Customs Act*
General checks for criminality	*Privacy Act* (s. 8)	Policy on the Disclosure of Information: s. 8 of the *Privacy Act*

Sources: CBSA, Review of CBSA National Security and Intelligence Activities: Joint Hearing with RCMP and CSIS, May 16, 2019; and Review of the CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.

Table 14: CBSA: Information sharing authorities and policy guidance

339. Information collected under the *Customs Act* may be used or shared for many purposes, including supporting national security and public safety priorities or administering and enforcing the following acts:

- IRPA for exercising the powers or performing the duties and functions of the Minister of Public Safety and Emergency Preparedness, including establishing a person's identity and determining that person's inadmissibility to Canada;
- the *Criminal Code* or for use in the preparation of criminal proceedings under an act of Parliament;
- the *Special Economic Measures Act* regarding the enforcement of economic sanctions;
- the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* regarding currency seizures and terrorism financing; and
- the *Export and Import Permits Act* relating to the movement of dual-use or restricted goods and technology.[50]

340. CBSA has a number of controls over the collection and sharing of information. The CBSA Chief Privacy Officer leads an internal centre of excellence on information sharing, which includes a 24/7 office to provide operational guidance to border services officers. CBSA also has a number of policy and operational guidelines to control information collection and sharing, including guidelines regarding the Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities, and policies on

[50] The *Customs Act*, s. 107(3-4).

information security, records retention and disposal. The Chief Privacy Officer works with the Office of the Privacy Commissioner to develop privacy impact assessments for CBSA operational activities.[51]

Immigration, Refugees and Citizenship Canada

341. CBSA works with IRCC at all points along the travel continuum to make admissibility evaluations and determinations for individuals seeking to enter Canada.[52] IRPA makes both the Minister of Immigration, Refugees and Citizenship and the Minister of Public Safety and Emergency Preparedness responsible for the administration of the Act.[53] IRCC is responsible for "facilitating the arrival of people and their integration into Canada in a way that maximizes their contribution to [Canada] while protecting the health, safety and security of Canadians." CBSA is responsible for "managing the flow of travellers at Canadian ports of entry, security screening, intelligence, interdiction of irregular migration and immigration enforcement. This includes responsibility for arrests, detentions, removals and representing [both Ministers] at hearings before the Immigration and Refugee Board."[54]

342. Under IRPA, CBSA conducts security screening on all cases referred to it, including incoming temporary or permanent resident applicants, and all adult refugee applicants, either abroad or at ports of entry. In this role, CBSA is the enforcement, intelligence and investigative arm of IRPA. CBSA also uses the IRCC database, the Global Case Management System, for aspects of its security screening risk assessment determinations, including for trusted traveller programs such as NEXUS.

343. CBSA and IRCC updated their memorandum of understanding (MOU) in 2017 to maintain a common understanding of the basis for cooperation on the implementation and delivery of programs and information sharing in support of various acts.[55] The MOU details the parameters and purposes for information sharing between the organizations, and the lawful authorities and policies under which the two organizations share personal information to fulfill their respective responsibilities.[56] The MOU states that CBSA and IRCC may share information where it is relevant to their respective jurisdictions and responsibilities related to national security, pursuant to SCISA, and defines the intelligence products, services and support that CBSA provides IRCC in regards to the immigration program.[57] Governance and oversight of the CBSA-IRCC relationship is provided through a deputy minister–level committee and sub-committees.

---

[51] CBSA, Review of the CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.
[52] CBSA, Statement of the Vice-President, Strategic Policy, NSICOP hearing, May 9, 2019.
[53] Government of Canada, *Ministerial Responsibilities Under the Immigration and Refugee Protection Act Order*, https://laws.justice.gc.ca/eng/regulations/SI-2015-52/page-1.html.
[54] CBSA, Memorandum of Understanding (MOU) between the Canada Border Services Agency and the Department of Citizenship and Immigration, February 2017.
[55] CBSA, Memorandum of Understanding between the Canada Border Services Agency and the Department of Citizenship and Immigration, February 2017. These Acts are: IRPA, the *Customs Act*, and the *Citizenship Act*.
[56] The MOU defines "Personal Information" as information about an identifiable individual that is recorded in any form as defined in section 3 of the *Privacy Act*. For the purposes of the MOU, "immigration", "citizenship", "passport", and "customs" information refers to Personal Information collected or compiled for these respective programs.
[57] Although SCISA has been replaced by SCIDA, the Committee has not received an updated MOU between CBSA and IRCC since SCISA was changed to SCIDA. In this case, the MOU shared with NSICOP references SCISA.

344. For this review, the Committee sought to identify challenges related to the organizations' shared responsibility for the administration and enforcement of IRPA. Both CBSA and IRCC stated that the authority basis for respective activities and responsibilities are clear. They described having a well-established governance structure that support complementary but distinct roles and responsibilities.[58]

345. Table 15 provides a breakdown of the CBSA-IRCC areas of cooperation on border-related activities that have national security outcomes.

Point in the Border Continuum	Activity Area	Collaborative Activities and Information Sharing	National Security Outcomes
Pre-border	Liaison officer network	• CBSA-IRCC information exchange in visa fraud • Detection and interdiction of document fraud • Collaboration on special operations (e.g., Operation Syrian Refugee) • Identification of improperly documented migrants	• Awareness of potential high-risk travellers or threats • Detection of high-risk inadmissible individuals
Pre-border and post-border	Immigration security screening	• IRCC referrals to CBSA for national security screening of immigration applicants and refugee claimants • CBSA provision of admissibility recommendations to IRCC • CBSA provision of national security assessments	• Recommendations to IRCC for inadmissibility under IRPA ss. 34, 35 and 37 • IRCC receipt of national security assessments to inform admissibility decision-making
Post-border	Intelligence and inland enforcement[59]	• Intelligence from confidential human sources • Removal of inadmissible individuals • CBSA support to Immigration and Refugee Board hearings	• Identification, detention or removal of high-risk, inadmissible individuals linked to national security risks

Source: CBSA and IRCC, Joint NSICOP hearing, May 9, 2019.

Table 15: CBSA-IRCC collaboration on border activities

[58] CBSA and IRCC, CBSA Vice-President of Strategic Policy and the IRCC Director General, Case Management Branch, Joint NSICOP hearing, May 9, 2019.

[59] Intelligence and Inland Enforcement activities include CBSA-led investigations, support to Immigration and Refugee Board hearings, IRPA related detentions, and removals of individuals deemed inadmissible pursuant to security-related sections of IRPA. CBSA and IRCC, Joint NSICOP hearing, May 9, 2019.

346. Immigration security screening is a collaborative process. Immigration security screening begins with IRCC's receipt of an application for permanent or temporary residency or refugee protection.[60] IRCC visa officers assess applications and may refer an applicant's file to CBSA or CSIS for further screening based on national security indicators, officer discretion or mandatory system referral requirements.[61]

347. When an application is referred to CBSA, its National Security Screening Division is responsible for screening applicants seeking temporary and permanent residence in Canada. It is also responsible for making recommendations of inadmissibility to IRCC, under IRPA sections dealing with terrorism, espionage and subversion, crimes against humanity and genocide, and organized criminality. In 2016-17, 2017-18 and 2018-19, respectively, CBSA provided IRCC with *** recommendations regarding individuals being inadmissible to Canada under subsection 34(1) of IRPA, which relates to terrorism, espionage and subversion. This represents approximately ***% of the total number of immigration security screening files that IRCC referred to CBSA in each year.[62]

The Royal Canadian Mounted Police

348. CBSA and the RCMP share responsibility for protecting Canada's borders through the administration and enforcement of the *Customs Act*, IRPA, the *Criminal Code*, and other relevant acts and regulations. CBSA and the RCMP established an MOU in 2014 to delineate their areas of shared responsibility and cooperation for border security. Both organizations report directly to the Minister of Public Safety and Emergency Preparedness.[63]

349. CBSA exercises its responsibilities at designated ports of entry. This includes "managing the flow of travellers and goods at [ports of entry], investigations of contraventions of the *Customs Act* and IRPA, and immigration enforcement activities."[64] The RCMP is responsible for investigations and monitoring the border between those designated ports, including primary responsibility for border security between and outside of ports of entry.[65] Cooperation between the RCMP and CBSA is strategic (development of policies, programs and procedures and program evaluation), operational (information sharing, providing mutual assistance) and tactical (joint operational activities and information sharing for specific investigations).

---

[60] The immigration security screening process can begin with an application received inside or outside Canada by an IRCC visa officer.

[61] The Global Case Management System (GCMS) will alert a visa officer if derogatory national security information exists in relation to an applicant. This information may be based on Canadian or allied information and intelligence, and can take the form of a national security lookout. IRCC visa officers and CBSA officers use lookouts as one piece of information to make admissibility determinations or recommendations. CBSA and IRCC officials described GCMS as "Canada's immigration system of record." Joint NSICOP hearing, May 9, 2019.

[62] CBSA and IRCC, Joint NSICOP hearing, May 9, 2019.

[63] CBSA and the RCMP, Memorandum of Understanding between the Royal Canadian Mounted Police and the Canada Border Services Agency, 2014.

[64] CBSA and the RCMP, Memorandum of Understanding between the Royal Canadian Mounted Police and the Canada Border Services Agency, 2014.

[65] CBSA and the RCMP, Memorandum of Understanding between the Royal Canadian Mounted Police and the Canada Border Services Agency, 2014; see also: CBSA, Royal Canadian Mounted Police, Statement of Cooperation, 2012.

350. The CBSA-RCMP MOU details divisions of responsibility and specific areas of cooperation and investigative responsibility related to border enforcement and administration, public safety, and support of national security outcomes. These include investigative responsibilities for counter proliferation, joint force operations and covert operations.

351. The MOU describes the authorities, parameters and conditions under which information can be shared between the organizations. CBSA may disclose information to the RCMP if it relates to accreditation of foreign visitors to major events held in Canada and customs information for criminal investigations, including information about the identity of a person, a commercial shipment or conveyance, or a *Customs Act* offence or seizure at the border.[66] The RCMP may disclose information to CBSA that is relevant to investigations or threats pertaining to the security of Canada; chemical, biological, radiological and nuclear incidents; critical infrastructure; proliferation of weapons of mass destruction; terrorism financing; threats against protected persons; and trafficking or smuggling of firearms, weapons, prohibited devices or ammunitions.[67] The RCMP may also provide CBSA with information relevant to other aspects of the CBSA mandate, including the security screening program, admissibility determinations under IRPA, the targeting of high-risk travellers, covert operations or controlled deliveries (that is, the intentional delivery of prohibited goods, intercepted at the border or elsewhere, to the intended recipient in order to identify or arrest the recipient or further a criminal or security investigation).[68]

The Canadian Security Intelligence Service

352. CBSA and CSIS share information on domestic and overseas cases to identify threats to the security of Canada and to assess admissibility under IRPA. In early 2015, CBSA and CSIS agreed to an MOU to identify "the basis for cooperation between the CBSA, which is responsible for administering and enforcing border-related legislation, and the CSIS in conducting national security investigations as well as sharing information in accordance with their respective mandates and applicable law."[69] In areas of joint operations, operational assistance and collaboration, the CBSA-CSIS MOU states that activities undertaken by each organization can "take the form of investigative techniques, the provision of equipment, the sharing of information, resources or personnel and the facilitation of conditions to allow the other Participant to safely and effectively meet its operational requirements."[70] The MOU further states that while activities conducted under the MOU may be performed jointly, or by one entity on behalf of the other, they must, in all cases, be subject to each organization's respective mandate and

---

[66] CBSA and Royal Canadian Mounted Police, Information Sharing Annex, Memorandum of Understanding, undated.
[67] CBSA and Royal Canadian Mounted Police, Information Sharing Annex, Memorandum of Understanding, undated.
[68] CBSA and Royal Canadian Mounted Police, Information Sharing Annex, Memorandum of Understanding, undated.
[69] CBSA and CSIS, Memorandum of Understanding between the Canada Border Services Agency and the Canadian Security Intelligence Service concerning an arrangement for ongoing cooperation on joint operations, operational assistance and collaboration as well as information sharing, April 2015.
[70] CBSA and CSIS, Memorandum of Understanding between the Canada Border Services Agency and the Canadian Security Intelligence Service concerning and arrangement for ongoing cooperation on joint operations, operational assistance and collaboration as well as information sharing, April 2015.

authorities. The CBSA-CSIS MOU notes that specific areas of cooperation (such as joint operations, areas of operational assistance and collaboration, and information sharing) will be identified in specific annexes to the MOU. Those annexes are expected to be finalized in 2019.[71]

International partnerships

353. The CBSA Act authorizes CBSA to enter into arrangements and agreements with foreign states and international organizations.[72] CBSA stated that the dynamism of border-related threats necessitates strong relationships with international partners. As a result, CBSA works with foreign counterparts to share best practices, tradecraft and, where applicable, intelligence, to facilitate admissible travellers and trade, and to identify those deemed high-risk and interdict if inadmissible. Of CBSA's many international partnerships, its relationships with the United States, the Border Five (B5) group of states (Canada, United States, United Kingdom, Australia and New Zealand), and the European Union are the most pertinent to this review of CBSA's national security and intelligence activities.

354. CBSA has strong relationships with American security agencies. In 1997, representatives of the governments of Canada and the United States signed an aide-memoire on procedures by which watch list data on suspected terrorists, derived from U.S. intelligence and law enforcement reports, may be shared with Canadian authorities responsible for visa operations and border security. Under this agreement, Canadian officials receive the names, dates of birth, passport numbers and nationalities (or countries of origin) of terrorist suspects listed on the U.S. Department of State's TIPOFF program.[73]

355. This Canada-U.S. agreement was later named TUSCAN (TIPOFF U.S.-Canada) and formalized in a 2016 arrangement. TUSCAN provides CBSA with information from the U.S. Terrorist Screening Center, including information related to Canadian citizens. [*** Three sentences were revised to remove injurious or privileged information. These sentences describe the sharing of information between Canada and the US under the TUSCAN agreement. ***][74] ***[75] ***[76]

356. Further to TUSCAN, CBSA shares information with the United States for a multitude of reasons across its Intelligence and Enforcement, Traveller and Commercial branches. As discussed in paragraph 384, CBSA shares information with U.S. Customs and Border Protection in the area of scenario-based targeting. Specifically, CBSA shares the biographical data of all travellers identified through a targeting scenario. In turn, U.S. Customs and Border Protection shares previous enforcement

---

[71] CBSA, How the CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019; and Statements of the CBSA Vice-President, NSICOP hearing, May 16, 2019.
[72] See *Canada Border Services Agency Act*, ss. 5(1)(*b*) and 13(2)(*b*).
[73] Canada and the United States of America, *Aide-Memoire. Concept of Operations: U.S.-Canada Terrorist Watch List Program*, May 23, 1997.
[74] CBSA, CBSA Information Sharing with the United States, March 16, 2018.
[75] CBSA, *** October 11, 2018.
[76] CBSA stated that TUSCAN information is one of many factors taken into consideration when making admissibility determinations. CBSA, Statements of the Director, Intelligence, Targeting and Criminal Investigations Program Management, NSICOP hearings, May 9 and May 16, 2019.

and travel history information on those individuals to inform CBSA's risk management process. CBSA may also share with its U.S. partners information related to immigration or high-risk travellers. Immigration-related information is shared on a case-by-case basis. CBSA shares information related to high-risk travellers with its American partners where there is a clear link to the United States. However, CBSA stated that this type of sharing is rare, as most CBSA high-risk traveller cases involve *Criminal Code* investigations of Canadian citizens and information would therefore be provided to the RCMP or CSIS.[77]

357. Beyond its bilateral relationship with the United States, the majority of CBSA's information-sharing is with the B5 group of states.[78] CBSA engages with its B5 counterparts in multiple fora to share tradecraft and best practices for border security. On scenario-based targeting, for example, [*** The rest of this sentence was revised to remove injurious or privileged information. The sentence names B5 fora for sharing. ***][79]

358. CBSA also works closely with counterparts in the European Union. In 2005, Canada and the European Community signed an agreement to ensure that Advance Passenger Information (API) and Passenger Name Record (PNR) data is provided consistent with fundamental rights and freedoms, including the right to privacy. The agreement commits both parties to process API/PNR data in accordance with applicable laws and constitutional requirements.[80] In 2014, Canada and the European Union added additional guidance on privacy protections and the provision and use of API/PNR data, including information related to police or judicial authorities.[81] In July 2019, Canada and the European Union concluded negotiations for a new PNR Agreement. Both parties have agreed to finalize the new Agreement following legal review.[82]

---

[77] CBSA, *CBSA Information Sharing with the United States*, March 16, 2018.
[78] CBSA, How the CBSA Uses Intelligence and Supports National Security Outcomes, Deck. Briefing to NSICOP Secretariat, January 10, 2019.
[79] CBSA, Operations Branch - National Border Operations Centre. National Targeting Centre. Briefing to NSICOP Secretariat, March 5, 2019.
[80] Canada and the European Community, *Agreement Between the Government of Canada and the European Community on the Processing of Advance Passenger Information and Passenger Name Record Data*, 2006.
[81] Canada and the European Community, *Agreement Between Canada and the European Community on the Transfer and Processing of Advance Passenger Information and Passenger Name Record Data*, June 25, 2014.
[82] Prime Minister of Canada, *Canada-EU Summit Joint Declaration*, July 18, 2019. https://pm.gc.ca/en/news/backgrounders/2019/07/18/canada-eu-summit-joint-declaration.

National security and intelligence activities

Mandate and the use of intelligence

359. As noted in the introduction, CBSA is best understood as an organization whose primary mandate is based on making admissibility decisions concerning goods and people and facilitating the flow of legitimate trade and travel; its national security responsibilities flow from that mandate. In the area of intelligence, CBSA conducts limited intelligence collection activities as part of a small program that supports operational activities across its full mandate.

360. CBSA's national security and intelligence activities support the organization's layered approach to risk assessment at each stage of the travel continuum. Three CBSA programs ***use*** or ***produce*** intelligence to support national security risk assessment needs:

- **Targeting program:** CBSA reviews pre-arrival information and intelligence for all travel modes to identify high-risk travellers and goods for examination upon arrival. This involves scrutiny of the movement of people and the shipment of goods, food, plants and animals.
- **Intelligence Collection and Analysis program:** CBSA collects, interprets and assesses intelligence to create and distribute actionable intelligence products (such as lookouts and bulletins) to its partners on the movement of people or goods across the border.[83]
- **Security Screening program:** Pursuant to IRPA, CBSA screens temporary resident and permanent resident applicants referred to it by IRCC, and all adult refugee protection claimants for admissibility determinations related to terrorism, espionage and subversion, and war crimes, crimes against humanity and genocide; and organized criminality. [84]

361. In addition to the program areas of Targeting, Intelligence Collection and Analysis, and Security Screening, several other CBSA programs can contribute to national security outcomes, including the following:

- **Immigration Enforcement:** This program involves activities such as investigations, detentions, hearings, and removals of foreign nationals and permanent residents who are, or may be, inadmissible to Canada, pursuant to IRPA, for reasons such as terrorism, subversion, war crimes, organized crime or serious criminality.

---

[83] This program collects and analyzes traveller and cargo information to develop actionable tactical, operational and strategic intelligence to support CBSA's operations and border enforcement mandate. CBSA collects intelligence through its detection and targeting tools and investigative techniques as mentioned in paragraph 362. See: www.cbsa-asfc.gc.ca/security-securite/irm-grr-eng.html.

[84] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat. January 10, 2019. A complete list of admissibility determinations is listed at ss. 34, 35 and 37 of IRPA.

- **Criminal Investigations:** CBSA pursues the investigation and prosecution of travellers, importers or other persons who commit criminal offences in contravention of Canada's border legislation.[85] Cases with national security implications are forwarded to the RCMP.
- **Traveller Facilitation and Compliance:** This includes the review of travellers' declarations and documentation prior to, or upon arrival at ports of entry to determine if travellers and their goods meet the requirements of applicable customs and immigration legislation and regulations. CBSA admissibility decisions may result in the interdiction of goods and persons of national security concern.
- **Commercial Trade Facilitation and Compliance:** This program includes interdicting non-compliant goods and conveyances at the border, monitoring admissible or controlled goods, and post-border compliance verifications, including export controls under the *Export and Import Permits Act*.[86]

362. CBSA conducts a number of national security and intelligence activities to support these programs. These activities (or tools) are:

- **detection and targeting tools**, which inform CBSA's risk assessments, and include radiation detector portals, biometric technology, small- and large-scale imaging, chemical trace detection technology, submersible cameras, and targeting activities, including scenario-based targeting;
- **investigative techniques and tools**, which support more detailed investigations and include surveillance, confidential human sources, lookouts, and joint force operations; and
- **the tools and activities of partners**, which include the intelligence activities and products of CSIS (human intelligence reporting), the Communications Security Establishment (signals intelligence reporting), the RCMP and CBSA's B5 partners.[87]

The Committee examines the most sensitive of these activities in paragraphs 368–430.

---

[85] Under the *Customs Act* or IRPA, this may include offences such as human smuggling, trade fraud, export fraud and contraband smuggling. CBSA, How the CBSA Uses Intelligence and Supports National Security Outcomes, Briefing to NSICOP Secretariat, January 10, 2019.

[86] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.

[87] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.

Expenditures on intelligence

363. Since 2015, CBSA has tracked its spending on intelligence as part of the National Security Expenditure Review, which was re-named the National Intelligence Expenditure Review in 2016–2017. CBSA's investments in supporting the government's implementation of the intelligence priorities are depicted in Table 16:

Year	Intelligence personnel (% of total CBSA personnel)	Total CBSA Personnel	Total expenditures on Intelligence Priorities (% of overall departmental expenditures)
2015–2016	*** (***%)	13,774	$*** (*** %)
2016–2017	*** (***%)	13,540	$*** (*** %)
2017–2018	*** (***%)	13,849	$*** (*** %)

Source: CBSA. 2015–2016, 2016–2017 and 2017–2018 submissions to the National Intelligence Expenditure Review.

Table 16: CBSA Expenditures on Intelligence Priorities 2015–2018

364. In addition to its resource expenditures in support of intelligence priorities, CBSA spent another $*** on its Integrated Enforcement and Intelligence Priorities, for a total of $*** ***% of total department expenditures in 2017–2018.[88] CBSA explained that the year-over-year increase in spending and personnel depicted in its National Intelligence Expenditure Review data is not a result of increases in the size of its intelligence program, but rather changes in calculation methodologies that included more program elements in later years.

Enforcement and intelligence priorities

365. In 2017, the Minister of Public Safety and Emergency Preparedness provided formal ministerial direction to CBSA to implement the government's intelligence priorities for 2017–2019.[89] The ministerial direction is meant to guide the alignment of CBSA's internal priorities, programs and resources with the government's Standing Intelligence Requirements. It also outlines the Minister's expectations for CBSA as it works to implement the intelligence priorities through the 2017–2019 cycle.[90] CBSA stated that its receipt of the ministerial direction was also meant to "reinforce Ministerial and [deputy ministerial] accountability and [to] create greater consistency within the Public Safety portfolio."[91]

---

[88] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019. CBSA explained that it has *** CBSA, Written Comments to NSICOP, July 5, 2019.

[89] See paragraph 104, NSICOP, *Annual Report 2018*, www.nsicop-cpsnr.ca/reports/rp-2019-04-09/2019-04-09_annual_report_2018_public_en.pdf.

[90] Additional information regarding the prioritization established by the government's intelligence priorities and the Standing Intelligence Requirements can be found in Chapter 3 of the NSICOP *Annual Report 2018* at: www.nsicop-cpsnr.ca/reports/rp-2014-04-09_annual_report_2018_public_en.pdf.

[91] CBSA, Written response to NSICOP questions, July 5, 2019.

366. Based on the Minister's direction, CBSA produced intelligence on a subset of the government's intelligence priorities for 2017–2019 in support of the CBSA mandate. Table 17 shows CBSA's areas of focus, its volume of intelligence reporting in response to the Minister's direction and its percentage of intelligence effort.

Government Intelligence Priority	Intelligence Reporting (April 2017 – June 2018)	Percentage of All Reporting
***	***	***%
***	***	***%
***	***	***%
***	***	***%
***	***	***%
Total	9,252	100%

Sources: CBSA, *** April 17, 2019; and CBSA, *** CBSA intelligence products include intelligence alerts, lookouts, intelligence briefs, intelligence advisories, intelligence bulletins, intelligence analysis, threat assessments and threat analysis reports.

Table 17: CBSA Intelligence Production (April 2017 – June 2018)

367. Internally, CBSA has developed a tiered prioritization scheme for its enforcement and intelligence programs.[92] These enforcement and intelligence priorities apply to CBSA's relevant enforcement and intelligence programs, which allocate a higher proportion of enforcement and intelligence resources to higher-risk threats and higher-level requirements (see Table 18). Although the Minister's direction identifies *** as priorities for CBSA, CBSA's enforcement and intelligence priorities do not address them directly. Rather, CBSA stated that "these threats have not been established as standalone [enforcement and intelligence] priorities but are considered aggravating factors when assessing the level of harm associated with offences under [either IRPA or the *Customs Act*] and [where] the priority of that offence is elevated; referral to the RCMP would normally be required."[93]

[92] CBSA, Integrated Enforcement and Intelligence Priorities 2017/18 – 2019/20.

[93] CBSA, Integrated Enforcement and Intelligence Priorities 2017/18 – 2019/20. See also: CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7 and May 9, 2019.

Tier	Percentage of Intelligence Resources Dedicated	Priorities
1	*** %	• *** • *** • *** • ***
2	*** %	• *** • *** • *** • ***
3	*** %	• *** • *** • ***[94] • ***
4	*** %*	• *** • *** • *** • ***

Source: CBSA, Integrated Enforcement and Intelligence Priorities 2017/18 – 2019/20.

* CBSA stated that its Tier 4 priorities are addressed through CBSA's normal border-related operations and border enforcement efforts, and thus do not receive dedicated intelligence resources.

Table 18: CBSA Enforcement and Intelligence Priorities 2017–2020

[94] Level 4 seizures meet or exceed a threshold of $10,000.

Sensitive national security and intelligence activities

368. Of the many tools and activities employed by CBSA, the Committee focused its review on CBSA's most sensitive security and intelligence activities due to their associated risks, including risks to privacy and human rights. These activities are scenario-based targeting; surveillance; confidential human sources; lookouts; and joint force operations. The Committee examines each of these activities in turn by describing the authorities under which they are conducted, the governance structures to which they are subject, the risks they pose and the results they produce.

Scenario-based targeting

369. CBSA identified scenario-based targeting as a program that uses or produces intelligence to support risk assessment efforts.[95] Scenario-based targeting identifies high-risk people, goods and conveyances bound for Canada that *may* pose a security threat. Using scenarios, CBSA conducts pre-arrival risk assessments for air passenger, air cargo, marine cargo, marine crews and vessels, highway cargo, and cruise ships, with planned expansion to commercial rail.[96]

370. Scenarios are computer-based algorithms. CBSA creates scenarios of high-risk patterns of travel based on information from CBSA's own programs and intelligence from Canadian and allied organizations. Scenarios are compared against passengers' biographical information and travel itineraries, which are provided to CBSA in advance by transport service providers, and manually assessed by targeting officers.[97] When officers cannot negate an identified risk through their assessment, they notify the port of entry, which refers the passenger to a mandatory secondary examination. This process is known as scenario-based targeting.

371. Targets are not indicative of the culpability of their subject. Rather, they are risk management tools that signal to border services officers that particular people, goods and vessels may pose a threat to the security and safety of Canada.

Authority for scenario-based targeting

372. CBSA stated that its authority to conduct scenario-based targeting is found in the CBSA Act, the *Customs Act,* IRPA and various regulations.[98] As noted in paragraph 326, the CBSA Act authorizes CBSA to support national security and public safety priorities, facilitate the free flow of persons and goods, and administer and enforce its program legislation. Together, IRPA and the *Customs Act* require that all

---

[95] CBSA, How the CBSA Uses Intelligence and Supports National Security Outcomes, Briefing to the NSICOP Secretariat, January 2019.

[96] CBSA, Operations Branch - National Border Operations Centre. National Targeting Centre. Briefing to NSICOP Secretariat, March 5, 2019.

[97] Biographical information provided by air carriers includes information such as name, date of birth, citizenship, passport and travel document number. This is generally the information found on page 2 of a Canadian passport. CBSA also receives commercial information from air, highway, marine and rail carriers, as well as freight forwarders and warehouse operators.

[98] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.

goods, persons and conveyances are reported to a CBSA officer, who is authorized to make admissibility decisions for both persons and goods. Scenario-based targeting allows officers to manage risk by focusing this lawful authority on goods, persons and conveyances that are of high-risk of non-compliance with CBSA's program legislation.

373. Pursuant to *Customs Act* regulations and IRPA, the owner or person in charge of a vessel must provide CBSA with advance information about the vessel itself and the persons and goods on board or expected to be on board.[99] The scenario-based targeting program uses information collected under these authorities.[100] These obligations apply to commercial transporters of passengers travelling by air, marine and rail.[101]

Governance of scenario-based targeting

374. In 2010, CBSA established the National Targeting Program as the functional authority to provide direction for all targeting activities. Following a phased implementation of a centralized National Targeting Business Model, CBSA established the centralized National Targeting Centre in 2012.[102] The establishment of the National Targeting Program was driven primarily by the desire to reduce the duplication of targeting efforts and to establish national standards for targeting across the various travel modes.[103] Scenario-based targeting is consistent with the targeting methodologies used by other B5 countries.[104] CBSA's international partnerships are discussed in paragraphs 353–358.

375. Scenario-based targeting is conducted within the National Targeting Centre, which operates 24 hours per day, 7 days a week within the National Border Operations Centre. *** the Canada Revenue Agency and U.S. Customs and Border Protection have an on-site presence at the National Targeting Centre, allowing for collaboration and support of the Targeting Program.[105] Governance of CBSA's Scenario Based Targeting Program is provided by the Enforcement and Intelligence Program Management Table, chaired by the Director General of the Intelligence and Enforcement Directorate. The Table is accountable to CBSA's Program Policy Committee, which reports in turn to the CBSA Executive Committee on strategic policy and program delivery.[106]

---

[99] *Customs Act*, s. 12.1 and s. 107.1; and IRPA, s. 148.
[100] CBSA Act, s. 2, s. 5; *Customs Act*, s. 159; IRPA, s. 34 (1)(*a*)–(*f*).
[101] *Passenger Information (Customs) Regulations*, s. 5(a)-(f); *Immigration and Refugee Protection Regulations*, s. 269(1)(*a*)–(*f*).
[102] CBSA, Enforcement and Intelligence Programs Directorate, Programs Branch, National Targeting Business Model, November 2014.
[103] CBSA, Enforcement and Intelligence Programs Directorate, Programs Branch, National Targeting Business Model, November 2014.
[104] CBSA, Targeting Intelligence, National Targeting Centre, *Scenario Based Targeting, Standard Operating Procedures*, Version 1.1, April 1, 2016.
[105] CBSA, Targeting Intelligence, National Targeting Centre, *Scenario Based Targeting, Standard Operating Procedures*, Version 1.1, April 1, 2016. Currently, CBSA has two National Targeting Centre liaison officers embedded at the U.S. National Targeting Centre. CBSA also has one National Targeting Centre liaison officer embedded in the Australian targeting centre. CBSA, Responses to NSICOP questions, July 5, 2019.
[106] CBSA, Scenario-Based Targeting Governance Framework, March 15, 2018.

376. Two CBSA governance bodies manage the development and use of scenarios:

- **Targeting Program Management Committee:** This body is responsible to ensure the management of the Targeting Program is efficient, effective and operationally compliant with international agreements, and with legislative and regulatory requirements.[107] It reports quarterly to the Enforcement and Intelligence Program Management Table.[108]
- **Scenario Management Committee:** This body is responsible to ensure that scenario-based targeting is effective and complies with privacy, legislative and regulatory requirements. Significant issues are escalated to the Targeting Program Management Committee where necessary.

Risks in targeting activities

377. CBSA acknowledges its use of scenario-based targeting comes with risks. CBSA stated that controls are in place to mitigate these risks, as outlined in Table 19 below:

Risk Type	Mitigation
Improper access to passenger data in CBSA systems	Data access is restricted to designated, trained personnel at the National Targeting Centre.
Inconsistent guidance or policy on targeting	Policy guidance is centralized in the Targeting Program at the National Targeting Centre.
Inadequate coordination of CBSA targeting efforts	Management committees meet regularly and are responsible for targeting program.
Improper access to targeting information by embedded personnel at the National Targeting Centre	Interdepartmental agreements control data access. Embedded staff have no access to CBSA data systems.

Source: CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.

Table 19: CBSA Targeting Program risks and governance controls

378. CBSA also acknowledged that scenarios in the air mode may infringe the civil liberties or human rights of travellers due to their reliance on API/PNR data from air carriers.[109] Consistent with relevant acts and agreements, CBSA takes measures to ensure that scenarios do not contain information that could reveal passengers' racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information about their sex life. As examples, scenarios may not include

---

[107] CBSA, Scenario-Based Targeting Governance Framework, March 15, 2018.

[108] CBSA, Audit of National Targeting Management Response and Action Plan, Draft, December 2015.

[109] CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019. Advance Passenger Information (API) includes an individual's name, date of birth, gender, citizenship and travel document data (e.g., passport number), as well as flight information such as a traveller's flight number and arrival and departure times. Passenger Name Record (PNR) data originates from, and differs by, airline. This information can include: type of ticket, date of travel, number of bags and seating information. See: www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/api_pnr_apt-ipv_dp_cpa-eng.html.

information on passengers' meal preference, family status, disability requirements, language, passport designation or birthplace.[110]

379. Sections of the *Protection of Passenger Information Regulations* govern the retention, use and disclosure of PNR information.[111] Target records are retained by CBSA for 10 years, and are available only to specified employees of the National Targeting Centre. The records are not available to front-line CBSA officers at a port of entry.[112]

Scenario development

380. CBSA takes a number of steps to develop scenarios. Scenarios are informed by previous enforcement actions, documented intelligence shared by national and international intelligence and targeting partners, and information stemming from security incidents or events. This can include ***[113] In addition, when targeting scenarios are proposed, targeting officers must include the specific statutory authority that supports the creation of the scenario.[114]

381. Scenarios fall within three main categories:

- **National security:** concerning terrorism and terrorist financing;
- **Immigration:** concerning non-genuine visitors, inadmissible persons, human smuggling/trafficking and previous deportations; and
- **Contraband:** concerning illicit drugs, weapons, proceeds of crime (currency smuggling), obscene material, and child exploitation material.[115]

382. The National Targeting Centre has identified *** as its highest priorities.[116] CBSA has tracked national security scenarios in the targeting program since 2013–2014 (see Table 20).[117]

---

[110] API/PNR data contains sensitive information for which a person would have a high expectation of privacy. The use and subsequent disclosure of this data is therefore protected under the *Privacy Act*, the *Customs Act*, the *Access to Information Act*, and the *Canadian Charter of Rights and Freedoms*. The data is also subject to Canada's international agreements, most notably the Canada-European Union Passenger Name Record Agreement.

[111] *Protection of Passenger Information Regulations*, s. 2-8.

[112] CBSA, Written response to NSICOP Secretariat questions: Question 4(d)(v), March 1, 2019.

[113] CBSA, Targeting Program, Enforcement and Intelligence Programs Directorate, Programs Branch, Scenario-Based Targeting Governance Framework, March 15, 2018.

[114] CBSA, Operations Branch - National Border Operations Centre. National Targeting Centre. Briefing to NSICOP Secretariat, March 5, 2019; CBSA, Targeting Intelligence, National Targeting Centre, *Scenario Based Targeting: Standard Operating Procedures*, Version 1.1, April 1, 2016.

[115] CBSA, Targeting Intelligence, National Targeting Centre, *Scenario Based Targeting, Standard Operating Procedures*, Version 1.1, April 1, 2016.

[116] CBSA, National Targeting Centre, NTC Priorities, March 2018.

[117] CBSA, Agency Performance Summary, Programs and Performance Q4 2015-16, Enforcement and Intelligence Dashboard, June 2016; and CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat, January 10, 2019.

Fiscal Year	Total Scenarios	Total National Security Scenarios	National Security as % of Total
2013–2014	31	***	***%
2014–2015	390	***	***%
2015–2016	467	***	***%
2016–2017	515	***	***%
2017–2018	558	***	***%
April 1, 2018 – Feb 26, 2019	542	***	***%

Source: CBSA, Written response to NSICOP Secretariat questions: Question 4(d)(ii), March 1, 2019; and CBSA, Written response to NSICOP Secretariat questions: Question 1, July 5, 2019.

Table 20: CBSA national security scenarios in the Targeting Program

383. Proposed scenarios are subject to multiple stages of analysis and approval before use. First, CBSA analyzes each scenario against historical data to understand how many targets the scenarios may produce and, consequently, whether scenarios require narrowing or broadening. Scenarios are reviewed for traveller impact and to ensure adherence to statutory and regulatory requirements.[118] If a violation of civil liberties, privacy or human rights is identified, the National Targeting Centre is notified to discuss resolution and engages senior management as required.[119]

Example of scenario-based targeting in practice

384. CBSA uses scenario-based targeting in the air passenger mode to identify potentially high-risk individuals travelling by plane to Canada. For this travel mode, CBSA obtains API/PNR from air carriers. CBSA then runs this data against scenarios to identify matches or "hits." CBSA targeting officers manually review these hits in order to assess and, where applicable, negate risk. This review consists of mandatory queries of internal and partner databases and open sources, a review API/PNR information, and consultation with other units within CBSA for information to confirm or deny a possible risk. Where risk cannot be negated for an individual hit, targeting officers proceed to a comprehensive review, comprising additional system queries. For national security targets, mandatory consultation with CSIS, the RCMP, U.S. Customs and Border Protection, and the Canada Revenue Agency is required.[120]

385. If risk cannot be negated by targeting officers, a target is issued, resulting in the mandatory referral of the passenger for secondary examination on entry, for customs or immigration purposes, or both. During this examination, border services officers rely on information obtained through the scenario-based targeting process to conduct the examination and to further assess risk. Following the

---

[118] CBSA described this stage as a measure of impact on the efficiency of the border process. A scenario may be viewed as ineffective if it creates a bottleneck of travellers being redirected to secondary examination. CBSA, Briefing to NSICOP, March 5, 2019.

[119] CBSA, Targeting Program, Enforcement and Intelligence Programs Directorate, Programs Branch, Scenario-Based Targeting Governance Framework, March 15, 2018.

[120] CBSA, Part 3, Chapter 1: Targeting Policy and Procedures, *Customs Enforcement Manual*, October 25, 2016.

examination, border services officers are required to enter the results of their examination into the Integrated Customs Enforcement System (ICES).[121]

Scenario-based targeting results

386. CBSA's use of scenario-based targeting has had an important impact on national security by identifying otherwise unknown individuals of national security concern (see Table 21).

	April 2015 – March 2016	April 2016 – March 2017	April 2017 – March 2018
Targets assessed for national security	687	843	829
National security targets of interest	349	395	409
Subjects of interest to CSIS	***	***	***
Subjects of interest referred to CSIS (unknown individuals)	***	***	***
Targets of interest to the RCMP	***	***	***
Targets referred to the RCMP (unknown individuals)	***	***	***
Targets of interest to U.S. Customs and Border Protection	***	***	***
Targets referred to U.S. Customs and Border Protection	***	***	***

Sources: CBSA, National Border Operations Centre, *National Security Targeting Monthly Report – March 2016*; CBSA, National Border Operations Centre, *National Security Targeting Monthly Report – March 2017*; and CBSA, National Targeting Centre, *National Targeting Centre Targeting Intelligence Monthly Report 2017–18.*

Table 21: CBSA Scenario Based Targeting - National Security Results

387. Table 22 illustrates the year-over-year impact for CSIS of CBSA national security information sharing (from the Targeting Program).

	April 2015 – March 2016	April 2016 – March 2017	April 2017 – March 2018
CSIS files impacted	***	***	***
CSIS existing files advanced	***	***	***
Previously unknown national security concerns identified	***	***	***

Sources: CBSA, National Border Operations Centre, *National Security Targeting Month Report – March 2016*; CBSA, National Border Operations Centre, *National Security Targeting Month Report – March 2017*; and CBSA, National Targeting Centre, *National Targeting Centre Targeting Intelligence Monthly Report 2017–18.*

Table 22: CBSA Targeting Program – Sharing with CSIS and national security results

[121] CBSA, Operational Bulletin: PRG-2017-19, Closing the Loop for Lookouts and Targets in the ICES; Operational Bulletin, May 3, 2017.

Surveillance activities

388. CBSA defines "surveillance" as "the **covert** observation of persons, vehicles, places or other objects to obtain information about individuals or organizations, where there are reasonable grounds to suspect they are in contravention of legislation administered by the CBSA." (emphasis in the original)[122] CBSA conducts surveillance activities to acquire or corroborate information that may lead to a direct enforcement action (e.g., execution of a removal order) or other activities such as arrests, lookouts, seizures of goods, obtainment of search warrants or referrals to other security partners.[123] Surveillance is only conducted within Canada and as part of inland enforcement operations.

389. For CBSA, surveillance includes:

- observing a house, place of business or other location to identify associates of a target, or to observe conveyances being used by a target and their associates;
- conducting site visits where officers use deception by pretending to be a fictitious person and make fictitious enquiries to obtain information for a CBSA investigation;
- following or observing a target to gather information on patterns of behaviour or movement to obtain evidence of suspected illicit activities, confirm suspicions of contraband smuggling or other illicit activities, or to locate contraband;
- following a target vehicle in order to install a court-authorized tracking device;
- following or observing a target to gather information that will assist in developing reasonable and probable grounds for an arrest or search warrant;
- following or observing a target to obtain detailed location information in preparation for the execution of a search or arrest; and
- following or observing a target to confirm information supplied by a source or from a tip.[124]

Authorities for conducting surveillance activities

390. CBSA stated that its authority to conduct surveillance activities can be found in the CBSA Act and the *Interpretation Act*.[125] As noted in paragraph 326, the CBSA Act provides CBSA with a mandate to provide integrated border services that support national security and public safety priorities, facilitate the free flow of persons and goods, and administer and enforce its program legislation. CBSA officers derive a common law authority, via the *Interpretation Act*, to engage in activities such as surveillance to accomplish the agency's enforcement mandate. CBSA's authority to conduct surveillance is limited by the *Canadian Charter of Rights and Freedoms*, CBSA's *Code of Conduct*, provincial traffic regulations, and other applicable legislation and policy.[126]

---

[122] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[123] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Presentation to NSICOP Secretariat. January 10, 2019. See also: CBSA, *Report on National Surveillance Operations: Fiscal Year 2017–2018*, 2018.
[124] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[125] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.
[126] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.

Governance of surveillance activities

391. CBSA's surveillance activities are governed by a formal Surveillance Policy. The policy stipulates that only select CBSA intelligence officers, investigators and inland enforcement officers are authorized to conduct surveillance activities. Those officers must complete mandatory surveillance training and certifications, and occupy positions where participation in surveillance operations is required. CBSA can conduct surveillance activities only within Canada.[127] The Surveillance Policy also requires CBSA to have reasonable grounds to suspect that a specific target is involved in the contravention of CBSA program legislation. This suspicion must be associated with a specific individual: CBSA cannot conduct surveillance if it only has grounds to suspect that contraventions of its program legislation are occurring in a particular place or in association with a particular activity.[128]

392. CBSA's surveillance activities are part of the Enforcement and Intelligence Program. In contrast to the governance architecture for scenario-based targeting, CBSA's surveillance operations are not subject to the oversight of governance bodies dedicated only to surveillance. Rather, the Surveillance Policy dictates that senior CBSA officials approve surveillance activities. The Surveillance Program is reviewed by CBSA's National Surveillance Coordinator, who reviews all approved surveillance plans and summary reports of all surveillance activities for policy and legal compliance, issue identification and resolution, performance, and costs.[129]

393. The Surveillance Policy states that approval levels for surveillance activities differ by level of expected risk. At a minimum, surveillance activities require the approval of a regional director. Surveillance activities that involve Canadian fundamental institutions – which include religious institutions, hospitals, women's shelters and post-secondary institutions – are considered higher risk and require a higher level of approval.[130] Specifically, all operations involving surveillance *of the perimeter* of a Canadian fundamental institution require the approval of the regional director general, while all operations involving surveillance *in* a Canadian fundamental institution require the approval of the Vice-President, Intelligence and Enforcement.[131] In exceptional circumstances that require an immediate response, CBSA officers may verbally brief senior officials and obtain approval to conduct surveillance. Such cases require CBSA officials to complete written surveillance proposals and approvals as soon as possible, and do not apply to surveillance involving Canadian fundamental institutions.[132]

---

[127] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[128] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[129] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019; and CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[130] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014. CBSA notes that Canadian fundamental institutions also include institutions of "heightened public sensitivities," although this term is not defined. CBSA gave the example that surveillance of a member of a bar or judiciary, even as an associate of a target, would be considered sensitive due to the potential for interference with the lawyer-client relationship or the independence of the judiciary.
[131] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.
[132] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014.

Risks in the use of surveillance

394. There are inherent risks in the conduct of surveillance activities. CBSA has adopted a number of measures to mitigate these risks. Risks and associated mitigation measures are depicted in Table 23.

Risk Type	Mitigation
Surveillance breaches an individual's reasonable expectation of privacy (REP)	REP Assessments are mandatory. Where an REP exists, a warrant for surveillance activity is required.
Surveillance undermines the integrity of a Canadian fundamental institution	Surveillance Policy provides guidance on Canadian fundamental institutions and requires heightened approvals and oversight.
Surveillance causes harm due to untrained personnel or nature of operations	Surveillance Policy requires specialized training and designation. Surveillance Policy requires training in defensive tactics and defensive equipment.
Surveillance operations receive inadequate or inconsistent oversight	Surveillance Policy requires a National Surveillance Coordinator (NSC) to review all plans and report for policy and legal compliance.
Surveillance operations are subject to inadequate or inconsistent interpretation of policy	The NSC reviews all training standards and policy interpretation. CBSA Legal Services provides legal advice for operations, when requested.

Source: CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.

Table 23: CBSA: Surveillance risks and governance controls

395. All proposals for surveillance operations must include an assessment of a reasonable expectation of privacy.[133] This assessment is designed to determine whether the target of surveillance operations has a subjective expectation of privacy, and whether that expectation is reasonable. CBSA conducts this assessment *before* a proposed surveillance operation and *during* ongoing operations, because an individual's reasonable expectation of privacy is context-specific and can change over time.[134] Officers must withdraw from surveillance activities if there is an unacceptable risk to any person or if a person's reasonable expectations of privacy may be infringed.[135]

396. CBSA does not require a warrant to engage in surveillance where a target has no reasonable expectation of privacy. Conversely, it must obtain a warrant to engage in a surveillance activity where a

---

[133] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January 2014. CBSA defines "reasonable expectation of privacy" as the objectively reasonable expectation or belief by an individual that their activity in the particular circumstances of a given situation is private and will not be the subject of government intrusion or information gathering, including surveillance. The test is whether a reasonable and informed person would expect privacy in the entire context of the situation.

[134] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January, 2014.

[135] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January, 2014.

target has a reasonable expectation of privacy.[136] Warrants may be issued only if there are reasonable grounds to believe that a specific offence is involved.[137]

Results

397. Since fiscal year 2015–2016, CBSA has produced annual reports on its surveillance operations. These reports summarize the number of approved surveillance operations conducted within each region, and include the area of focus of operations (smuggling and contraband, immigration fraud, irregular migration and national security), associated costs and results. See Table 24.

	2015–2016	2016–2017	2017–2018
Number of surveillance operations	***	***	***
Surveillance operations related to national security (% of all surveillance operations)	***	***	***
Resources expended for surveillance operations	***	***	***

Sources: CBSA, *Annual Report on National Surveillance Operations, Fiscal Year 2015–2016*; CBSA, *Report on National Surveillance Operations: Fiscal Year 2016–2017*; and CBSA, *Report on National Surveillance Operations: Fiscal Year 2017–18*.

Table 24: CBSA: Surveillance Results

[136] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January, 2014.
[137] CBSA, Part 3: Selection, Chapter 6: Surveillance, *CBSA Enforcement Manual*, January, 2014.

Confidential human sources

398. CBSA defines confidential human sources as individuals who:

- are willing to provide information of value, related to the mandate of the CBSA, that cannot be easily obtained through other sources;
- indicate to a CBSA employee that they wish their identity to be treated confidentially; and
- after a positive CBSA evaluation, receive an assurance of confidentiality from a certified CBSA confidential human source (CHS) officer and are registered within CBSA as a CHS Program participant.[138]

399. CBSA's use of confidential human sources dates to 1984.[139] CBSA stated that confidential human sources are not agents and that the distinction between a "human source" and an "agent" is critical. For CBSA, a confidential human source is a person who volunteers information to CBSA and who requests and receives assurances that their identity be treated confidentially. That confidentiality is a near-absolute privilege recognized by the courts.[140] In contrast, an agent is "a person who acts on the direction of a law enforcement officer to assist in the development of a target operation." Agents are not protected by informant privilege.[141] CBSA does not work with agents and it does not direct its sources to act on its behalf. As discussed in paragraph 405, CBSA may co-handle a confidential human source with another law enforcement organization in the context of a joint force operation, but CBSA would terminate its relationship with the source if he or she became an agent for that organization.

400. CBSA does not promise ongoing payment for information from its confidential human sources. CBSA may provide monetary "awards" to confidential human sources whose information leads to significant enforcement actions.[142] CBSA stated that its financial authority to issue monetary awards to confidential human sources stems from its legal authority to investigate contraventions of program legislation and from its authority under Part III of the *Financial Administration Act* to expend money in accordance with its law enforcement mandate.[143] The CBSA CHS Program operates only within Canada.[144]

401. As of 2014, CBSA tracked the use of confidential human sources in internal annual reports, including year-over-year changes in the number of registered CHS Program participants, regional fluctuations in the use of confidential human sources, evolutions in the policy and governance structure

---

[138] CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, September 2014.
[139] CBSA, *Review of the Confidential Human Source (CHS) Program.* July 2014. See also CBSA, *2014–15 Annual Report, Confidential Human Source Program, Executive Committee Briefing*, August 20, 2015.
[140] CBSA, Response to NSICOP on questions regarding the distinction between an agent and a source, June 13, 2019.
[141] CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, September 2014; and CBSA, Response to NSICOP on questions regarding the distinction between an agent and a source, Email, June 13, 2019.
[142] CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, September 2014.
[143] CBSA, Response to NSICOP on questions regarding the distinction between an agent and a source, June 13, 2019, and CBSA, responses to NSICOP questions, July 19, 2019.
[144] CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, September 2014.

for the CHS Program, and the value and impact of enforcement actions taken as a result of information provided by such sources.

Authorities for the use of confidential human sources

402. CBSA stated that its authority for the recruitment, use and development of confidential human sources is the CBSA Act and the *Interpretation Act*.[145] As noted in paragraph 326, the CBSA Act provides CBSA with a mandate to provide integrated border services that support national security and public safety priorities, facilitate the free flow of persons and goods, and administer and enforce its program legislation. The *Interpretation Act*, in turn, provides CBSA the authority to use confidential human sources to accomplish its enforcement mandate. The authority to use confidential human sources is also grounded in common law powers.

Governance of confidential human sources

403. CBSA stated that, prior to 2014, there had been no formal policy on the recruitment, development and management of confidential human sources, and no standard operating procedures in place to guide handlers and co-handlers in carrying out their duties.[146] In 2014, CBSA formalized its CHS Program and standardized its approach to the management, coordination and operational use of confidential human sources. The resulting CHS Policy and CHS Standard Operating Procedures define who may engage in activities with CHS Program participants (sources), how such activities will be conducted, and how engagements related to confidential human sources will be managed with other Canadian law enforcement agencies.[147]

404. The CHS Policy and CHS Standard Operating Procedures establish a graduated, risk-based framework to control the recruitment, approval, development and management of confidential human sources. As risk levels increase, the level of approval required for developing or managing an individual confidential source also increases. Control measures include obligations to officially register sources as CHS Program participants, requirements that only CBSA officers trained and certified as CHS officers may handle sources, and that in-person meetings with sources are conducted by two certified CHS officers and supported in every case by documented operational plans.[148]

405. The CHS Policy prohibits certain categories of individuals from being used as sources, including ***[149] The policy also requires special approval from the CBSA President for sources from potentially sensitive groups (such as a member of a Canadian fundamental institution) or former employees of a foreign law enforcement or intelligence organization; and from the CBSA Vice-President or Associate

---

[145] CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.
[146] CBSA, *Review of the Confidential Human Source (CHS) Program*, July 2014. See also, CBSA, *2014–15 Annual Report, Confidential Human Source Program, Executive Committee Briefing*, August 20, 2015.
[147] CBSA, Part 3, Selection, Chapter 7, Confidential Human Source Policy, *CBSA Enforcement Manual,* September 2014.
[148] CBSA, Part 3, Selection, Chapter 7, Confidential Human Source Policy, *CBSA Enforcement Manual,* September 2014.
[149] CBSA, Part 3, Selection, Chapter 7, Confidential Human Source Policy, *CBSA Enforcement Manual,* September 2014.

Vice-President of the Intelligence and Enforcement Branch in exceptional cases, currently used to approve the co-handling of sources with another law enforcement agency.[150]

406. The CHS Program is part of the Enforcement and Intelligence Program. The Enforcement and Intelligence Program is responsible for the "functional direction, application and monitoring of policy, legislation and jurisprudence, standard setting for training and the measure and reporting on national performance of the CHS Program."[151] It is also responsible for implementing and ensuring compliance with the CHS Policy, and ensuring that CBSA senior management is kept apprised of any operational issues that could affect the integrity of the CHS Program.[152]

Risks in the use of confidential human sources

407. In its CHS Policy, CBSA acknowledges that the use of confidential human sources can involve considerable risks.[153] Table 25 lists the risks and measures to mitigate them.

Risk Area	Mitigation
Inappropriate handling of a confidential human source leading to harm for a source, or handler	Confidential human source handlers receive special training and designation, and their activity is overseen by designated regional coordinators.
Confidential human source involvement in criminal activity	Risk assessments are required for each source; there is no engagement in proscribed categories.
A source as a member of a Canadian fundamental institution could undermine the institution or vulnerable populations	CHS Policy defines Special Approval categories, which require enhanced risk assessments and special approval procedures.
Inadequate oversight of the CHS Program	CHS Program is subject to CBSA regional and national oversight; a risk-based approval framework; formal policy guidance and standard operating procedures; and CHS Program reporting to CBSA management.
National inconsistency in CHS Program use	CHS Program centralized at CBSA headquarters since 2014; all handlers are specially trained.
Compromise of a confidential source due to CBSA mishandling information	CHS information is segregated on CBSA systems; access is strictly controlled.

Source: CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.

Table 25: CBSA Confidential Human Source Program; Risk Controls

---

[150] CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019. See also: CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, March 2016. The CHS Policy does not further define what would constitute an "exceptional circumstance."

[151] CBSA, *Review of the Confidential Human Source (CHS) Program.* July 2014.

[152] CBSA, *Review of the Confidential Human Source (CHS) Program.* July 2014.

[153] CBSA, Part 3: Selection, Chapter 7: Confidential Human Source Policy, *CBSA Enforcement Manual*, September 2014. The *CBSA Enforcement Manual* delineates Special Approvals categories for CHS Program participants, all of which are subject to approval by the CBSA President.

Internal review of the CHS Program

408. The CHS Program has undergone two internal reviews: in 2014 and 2018. The 2014 review sought to assess risks associated with CBSA's authority to use confidential human sources, and the adequacy of the CHS Program design, guidance and operational procedures. The review found that CBSA's authority for the CHS Program was derived from its mandate and that CBSA "has the appropriate legislative basis to carry out the Confidential Human Source Program."[154] That said, given the sensitivities of the program, the review recommended that CBSA seek ministerial direction for CHS and other sensitive activities (this direction had been sought in 2013, but not provided). The review also stated that CBSA officers responsible for conducting CHS activities had expressed concerns about the absence of formal policies that described clear roles, responsibilities and accountabilities. It recommended that such policies be developed; they subsequently were.[155]

409. The 2018 review suggested that the absence of ministerial direction had caused uncertainty around CBSA's mandate and legal authority to conduct CHS activities over the previous five years.[156] [*** The following three sentences were revised to remove injurious or privileged information. The sentences note that the Committee understood that CBSA derived its authority to conduct CHS activities from its statutory law enforcement mandate.[157] ***][158] Nonetheless, the 2018 review noted that, "the lack of a clear program direction is limiting the extent to which CHS activities support CBSA's operations," and that obtaining ministerial direction was an opportunity to bring CBSA in line with other portfolio partners that have ministerial direction for their CHS activities, including the RCMP and CSIS.[159] The Committee addresses this issue in its findings.

Results

410. CBSA employs a financial methodology to assess the success of its CHS Program. In general terms, CBSA stated that the CHS Program assists "the Agency in obtaining critical intelligence that may not be otherwise available [and which adds] value to both tactical and strategic Agency intelligence and enforcement programs."[160] Specifically, CBSA evaluates the success of the program by a measure of "enforcement value" *** based on information provided from individual sources.[161] Table 26 illustrates the annual size of the CHS Program by the number of active, registered confidential human sources since 2014–2015, the number of enforcement actions based on the information they provided, and the dollar value that CBSA has placed on those enforcement results.

---

[154] CBSA, *Review of the Confidential Human Source (CHS) Program*, July 2014.
[155] CBSA, *Review of the Confidential Human Source (CHS) Program*, July 2014.
[156] CBSA, *Review of the Confidential Human Sources (CHS) Program: Draft Report*, February 2018.
[157] Supreme Court of Canada, *Canada (Citizenship and Immigration) v. Harkat*, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13643/index.do. See also paragraphs 331–332 regarding the *Interpretation Act*, and its role as an enabling authority for this activity.
[158] CBSA, *** February 2018.
[159] CBSA, *Review of the Confidential Human Sources (CHS) Program*, Draft report, February 2018.
[160] CBSA, *Review of the Confidential Human Source (CHS) Program*, July 2014.
[161] CBSA, Confidential Human Source Program, FY 2015–2016; and CBSA, Confidential Human Source Program, FY 2017–2018.

Year	Registered CHS Program Participants (active)*	Number of CHS-based Enforcement Actions	Enforcement Action Values
2014–2015	***	***	$***
2015–2016	***	***	$***
2016–2017	***	***	$***
2017–2018	***	***	$***

Source: CBSA. Data compiled from Confidential Human Source Program annual reports for the years 2014–15, 2015–16, 2016–17, and 2017–18.

* Yearly notations of active participants in the CHS Program represent the total active participants in the program up to that point. In any given year, CHS participants may be recruited and added as new sources, or deactivated and delisted as sources.

Table 26: Confidential Human Source Program. Size and Results Snapshot

411. CBSA also tracks how much it spends on awards for each CHS Program participant. It uses these expenditures and the calculated enforcement values (as shown in Table 26) to determine an overall return on investment for the CHS Program (see Table 27).

Year	CHS-based Enforcement Actions	Awards Issued (# of awards)	Enforcement Action Values	Return on Investment
2014–2015	***	$***	$***	***
2015–2016	***	$***	$***	***
2016–2017	***	$***	$***	***
2017–2018	***	$***	$***	***

Source: CBSA. *** various dates.

* ***

Table 27: CHS Program Return on Investment

Lookouts

412. Lookouts are an electronic record within CBSA's systems, and are a type of intelligence product that CBSA creates to improve its ability to manage risk at ports of entry. Unlike scenarios, which begin with trend analysis that is *informed* by intelligence, lookouts are, themselves, an intelligence product.

413. Lookouts are issued in relation to a particular person, corporation, conveyance or shipment that has a high risk of posing a threat to the health, safety, security, economy or environment of Canada or Canadians.[162] They signal to border services officers that particular goods, persons or conveyances are high risk and, in the case of active lookouts (see paragraph 414), they *must* be referred for a secondary examination.[163] Lookouts are a prompt for closer examination, not evidence that border-related legislation has been contravened.[164] Lookout information contains specific instructions for intercepting officers that allow them to take appropriate action, including precautions that intercepting officers should take to ensure their safety or to explain further reporting requirements.[165]

414. Following the secondary examination of lookouts, border services officers must input lookout examination results into the CBSA's Integrated Customs Enforcement System. This includes "any relevant information requested by the lookout originator and additional information, which must be within CBSA's legal authorities and mandate."[166] Lookouts can be issued by CBSA ***[167] Other government departments and agencies are responsible for the maintenance of lookouts issued on their behalf.[168] CBSA reviews lookouts prior to their expiration and may modify and extend them based on new information, the interception of the subject of the lookout and officer discretion.[169]

415. [*** This paragraph was revised to remove injurious or privileged information. The paragraph discusses types of lookouts. ***]

- ***
- ***[170]

---

[162] CBSA, *National Directive on Lookouts*, December 23, 2015.
[163] CBSA, *Audit of Lookouts – Traveller Mode*, June 2013.
[164] CBSA, *CBSA Lookout Policy*, June 2013.
[165] CBSA, National Directive on Lookouts, December 23, 2015.
[166] CBSA, Operational Bulletin: PRG-2017-19, Closing the Loop for Lookouts and Targets in the ICES; May 3, 2017.
[167] CBSA, *** June 2013.
[168] CBSA, *CBSA Lookout Policy*, June 2013. Unclassified; and CBSA, *Standard Operating Procedures (SOP): Lookouts*, June 2013.
[169] CBSA, *CBSA Lookout Policy*, June 2013.
[170] CBSA, *** November 28, 2011.

Authorities for the use of lookouts

416. CBSA stated that its authority to issue lookouts can be found in the CBSA Act and the *Interpretation Act*.[171] As noted in paragraph 326, the CBSA Act provides CBSA with a mandate to provide integrated border services that support national security and public safety priorities, facilitate the free flow of persons and goods, and administer and enforce its program legislation. CBSA officers derive their authority to employ tools such as lookouts to accomplish their enforcement mandate from an established common law doctrine, now codified in the *Interpretation Act* (see paragraphs 331-332).

Governance of lookouts

417. Governance for lookouts consists of assessments conducted by CBSA officers before lookouts are issued and monthly reviews of lookouts by senior management. Prior to issuing a lookout, CBSA officers must confirm it is consistent with the CBSA mandate and program legislation, and assess the relevance, reliability and credibility of the information on which it is based. To ensure compliance with lookout policies and procedures, senior management undertakes monthly reviews of the accuracy and validity of a sample of lookouts created and maintained by their staff.[172]

418. CBSA lookouts that involve other government organizations are governed by a number of acts and policies. If information collected as a result of a lookout is to be disclosed to other government organizations, it must be done pursuant to section 107 of the *Customs Act* or section 8 of the *Privacy Act*.[173] When lookouts issued by other government organizations would require border services officers to engage in questioning that extends beyond CBSA program legislation, a warrant is required.[174]

---

[171] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.

[172] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019. This was a response to a 2013 internal audit that found that oversight and ongoing monitoring of lookouts was limited.

[173] CBSA, *Standard Operating Procedures (SOP): Lookouts*, June 2013.

[174] CBSA, *Standard Operating Procedures (SOP): Lookouts*, June 2013.

Risks of lookouts

419. Table 28 lists the risks and mitigation measures CBSA identified related to its use of lookouts.

Risk	Mitigation
Lookouts not intercepted at ports of entry	CBSA's operational bulletins and policies make clear that border services officers are to refer all lookouts for a secondary examination.
Lookouts not entered into CBSA's systems on encounter at a port of entry	Operational bulletins state that border services officers must input lookout examination results into CBSA systems. Lookout results are examined at the end of each shift, ensuring that missing or incomplete examination results are followed up in a timely manner. Lookouts are sampled monthly for review to ensure compliance with policy and procedures.
Lookouts do not fall within CBSA's mandate and jurisdiction	CBSA officers must confirm that the issuance of a lookout aligns with CBSA's mandate and program legislation. In cases of disagreement over the issuance of a partner-requested lookout, the issue is raised to responsible managers and directors-general of each organization.
Improper use or disclosure of lookout information could infringe on a traveller's privacy rights	CBSA's system for managing enforcement-related information has a back-end auditing function that monitors access, allowing CBSA to ensure that there is no unauthorized access to lookouts. CBSA may share lookout information pursuant to s. 107 of the *Customs Act* and s. 8 of the *Privacy Act*. However, disclosure is discretionary; CBSA officials may refuse to disclose information for a variety of reasons including whether the disclosure compromises an ongoing investigation.

Source: CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019; and CBSA, Email response to NSICOP Secretariat, June 14, 2019.

Table 28: Lookouts: Risks and Mitigation Measures

Results of lookouts

420. As noted in paragraph 413, lookouts signal to border services officers that particular goods, persons or conveyances are high risk and (in the case of active lookouts) *must* be referred for a secondary examination.[175] As a prompt for closer examination, as opposed to a specific indicator of the contravention of border legislation, CBSA measures results for the use of lookouts in two ways. First, through a measure of the number of lookouts successfully intercepted – that is, the positive correlation of goods, persons, or conveyances with a specific lookout, and the divergence of that person, good or conveyance to secondary examination. The second measure of success for the use of lookouts is a measure of the number of secondary examination reports, or results, that are entered into CBSA systems, and which may feed additional information to CBSA intelligence officers and provide a proof of record for border services officer decision-making and interactions with travellers. CBSA stated it could not provide a disaggregated breakdown of its use of lookouts solely for national security purposes. As a result, no further details on the results of CBSA's use of lookouts is available.

[175] CBSA, *Audit of Lookouts – Traveller Mode*, June 2013.

Joint force operations

421. CBSA defines a joint force operation as "an ongoing or regularly occurring activity with law enforcement partners, either international or domestic, designed to reach well defined objectives that support the CBSA's mandate."[176] CBSA participates in joint force operations with federal, provincial, municipal and international partners to "leverage the combined expertise and resources of participating organizations to achieve common or complementary enforcement goals."[177]

422. CBSA engages in four types of national security-related joint force operations. These are:

- **Integrated National Security Enforcement Teams (INSETs):** Located in major cities across Canada, INSETs are led by the RCMP to ensure a coordinated approach to investigating the activities of individuals or organizations that pose a threat to national security by sharing federal, provincial and municipal resources.[178]
- **National Security Joint Operations Centre (NS-JOC):** The NS-JOC coordinates the government's response to high-risk travellers or individuals, provides intelligence support to INSETs, and collocates analysts from participating agencies.
- **Integrated Border Enforcement Teams (IBETs):** IBETs are Canada-U.S. inter-agency teams that identify, investigate and combat cross-border criminal activity and security threats.
- **Marine Security Operations Centres (MSOCs):** MSOCs co-locate personnel from CBSA, Fisheries and Oceans Canada, the Canadian Coast Guard, the RCMP, Transport Canada, and the Department of National Defence to respond to national security threats in the marine environment.[179]

Authorities for joint force operations

423. CBSA stated that its authority for participating in joint force operations is the CBSA Act and the *Interpretation Act*.[180] As noted in paragraph 326, the CBSA Act provides CBSA with a mandate to provide integrated border services that support national security and public safety priorities, facilitate the free flow of persons and goods, and administer and enforce its program legislation. CBSA officers derive a common law authority to leverage the shared resources and expertise of its partners (in a joint force environment) to accomplish the agency's enforcement mandate. Importantly, CBSA's authority to participate in joint force operations is limited to those circumstances where there is a direct connection to the CBSA mandate and program legislation. CBSA activity in a joint force environment is prohibited in all other circumstances.[181]

---

[176] CBSA, Part 3, Chapter 8: Joint Forces Operations Policy, *Customs Enforcement Manual*, August 18, 2016.
[177] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Briefing for the NSICOP Secretariat, January 10, 2019.
[178] CBSA, How CBSA uses Intelligence and Supports National Security Outcomes, Briefing for the NSICOP Secretariat, January 10, 2018.
[179] CBSA, National Joint Force Operations Fiscal Year 2017–18, undated.
[180] CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.
[181] CBSA, Comments, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.

Governance of joint force operations

424. CBSA's participation in joint force operations is managed by a designated National Coordinator within CBSA's Intelligence and Enforcement Branch. The National Coordinator is responsible for reviewing all proposed joint force operations to ensure they are consistent with CBSA's policy, mandate and priorities and, when approved, are implemented according to the CBSA Joint Forces Operations Policy. The policy provides for a governance and internal oversight system consisting of internal approvals, reporting, review and formal agreements between CBSA and its partners.[182] The National Coordinator is also responsible for ensuring that each stage of a joint force operation remains consistent with CBSA's mandate, legislation and priorities. If an operation deviates from CBSA's mandate, legislation and priorities, CBSA ceases its participation.[183]

425. Before it can participate in a joint force operation, CBSA and its partners complete a Joint Forces Operation Agreement. This agreement has two components:

- **Joint Force Operation Assessment**, a management-approved, written description of the proposed activity, which must include provisions to assess and measure the performance of CBSA participation in the joint force operation; and
- **Joint Force Operation Written Collaborative Arrangement**, a document that establishes the parameters of a working partnership within a joint force operation and that complies with CBSA policy.[184]

The written collaborative arrangement defines the respective roles, responsibilities and authorities of each member.[185] CBSA stated that the Joint Forces Operation model permits it and its partners to identify and resolve challenges, and described joint force operations as "well-oiled machines."[186]

---

[182] CBSA, Part 3, Chapter 8: Joint Forces Operations Policy, *Customs Enforcement Manual,* August 18, 2016.
[183] CBSA, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.
[184] CBSA, Part 3, Chapter 8: Joint Forces Operations Policy, *Customs Enforcement Manual*, August 18, 2016.
[185] RCMP, Assistant Commissioner, Federal Policing Operations and CBSA, Director, Intelligence, Targeting and Criminal Investigations Program Management, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019. Both organizations noted that the roles, responsibilities and authorities are known, respected and understood by all parties involved.
[186] CBSA, Director, Intelligence, Targeting and Criminal Investigations Program Management, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.

Risks in joint force operations

426. There are risks associated with joint force operations. Table 29 lists the risks and measures to mitigate them.

Risk Area	Mitigation
Joint force operation is inconsistent with the CBSA mandate	All operations are subject to assessment and written agreement prior to CBSA involvement. All operations must support a CBSA enforcement and intelligence priority.
Inadequate oversight of joint operational activities	National Joint Force Operation Coordinator provides oversight, including through quarterly reports and annual review of activities.
Inadequate written agreements between partners	All joint force operation agreements are reviewed by the CBSA Chief Privacy Officer.
Inappropriate disclosure of CBSA information in the context of a joint force operation	All CBSA participants are trained and subject to disclosure policies. Written agreements ensure partners are aware of CBSA limits to participation.

Source: CBSA, Review of CBSA National Security and Intelligence Activities, Presentation to NSICOP, May 7, 2019.

Table 29: CBSA Joint Force Operations; Risk Controls

Measuring joint force operations results

427. CBSA performance in joint force operations and its return on investment is measured against the objectives set out in the Joint Force Operations Agreement.[187] CBSA began tracking performance metrics across all joint force operations in mid-2017, and Table 30 lists the results:

Joint Force Operations Results Measure	2017–2018	2018–2019
Investigative leads received from partners	***	***
Investigative leads generated for partners	***	***
Issued national security lookouts	***	***
Created lookouts and targets in CBSA data systems	***	***

Sources: CBSA, National Security Joint Operation Centre (NS-JOC), Briefing note, February 9, 2018; and CBSA, Written response to NSICOP Secretariat questions: Question 2, July 5, 2019.

Table 30: CBSA Joint Force Operation Results Measures, 2017-2019

[187] CBSA, Part 3, Chapter 8: Joint Forces Operations Policy, *Customs Enforcement Manual,* August 18, 2016; CBSA, CSIS and the RMCP, Review of CBSA National Security and Intelligence Activities, Joint NSICOP hearing with CBSA, CSIS and the RCMP, May 16, 2019.

The National Security Joint Operations Centre (NS-JOC) and high-risk travellers

428. The Committee further explored CBSA's efforts to identify and interdict high-risk travellers, a threat to which CBSA responds using the same tools and authorities which it relies upon to counter other border-related threats.[188] Just as it may do for all persons and goods seeking to enter Canada, CBSA may examine high-risk travellers and their goods to assess admissibility. If a border services officer finds evidence that points to an offence under the *Criminal Code* or under any other Act of Parliament during an examination, the officer may seize the evidence and detain the individual for transfer to the police of jurisdiction, pursuant to the *Customs Act*.[189] CBSA may also refer a Canadian suspected of being a high-risk traveller to CSIS, who may interview the individual, subject to that person's consent.[190] If there is not a direct connection to the CBSA mandate, CBSA officers cannot use these powers for the sole purpose of collecting evidence of an offence under the *Criminal Code* or of criminal offences under any other act of Parliament.[191]

429. CBSA also contributes to Canada's response to the threat of high-risk travellers through participation in the RCMP-led NS-JOC, which was established in October 2014 as a fusion centre for government departments and agencies with a direct stake in counter-terrorism and the identification and interdiction of high-risk travellers.[192] As of February 2018, the membership of NS-JOC included officials from the RCMP, CBSA, CSIS, IRCC, DND (the Canadian Forces National Investigation Service and Canadian Special Operations Forces Command), FINTRAC, the Communications Security Establishment, Global Affairs Canada, and the Canada Revenue Agency.[193] CBSA supports NS-JOC in the fulfillment of its objectives. NS-JOC's main objectives include:

- **Act as a centre of expertize specializing in national security investigations:** NS-JOC facilitates the sharing of best practices, investigative techniques and subject matter expertise.
- **Collect, analyze and disseminate intelligence among member agencies:** NS-JOC reports information and intelligence to member agencies, INSETs and RCMP National Security Enforcement sections.
- **Review and coordinate a whole-of-government response to emerging issues:** For example, NS-JOC monitors and reports on the number of returned foreign fighters.[194]

CBSA's role within NS-JOC is also to "share relevant information with NS-JOC members regarding high-risk travellers and high-risk individuals, such as watch list and lookout information, in accordance with the relevant sections of the *Customs Act* and the *Privacy Act*."[195]

---

[188] CBSA, The Role of the CBSA in Identifying & Reporting High Risk Travellers, 2014.
[189] *Customs Act*, ss. 163.5(1), ss. 163.5(3).
[190] CBSA, High-Risk Traveller Initiative, Technical Panel – Legislative Authority Review, 2016.
[191] *Customs Act*, ss. 163.5(4).
[192] CBSA, *Emergency Response Procedures – NSJOC*, November 2016.
[193] CBSA, National Security Joint Operation Centre (NS-JOC), Briefing note, February 9, 2018; and RCMP, Feedback to NSICOP, July 5, 2019.
[194] CBSA, National Security Joint Operation Centre (NS-JOC), Briefing note, February 9, 2018.
[195] RCMP, Terms of Reference: National Security Joint Operations Centre, March 1, 2015.

430. CBSA has also established a high-risk traveller team as part of an interdepartmental high-risk traveller initiative. The team comprises subject matter experts who serve as the central point of contact for front-line operations and partner agencies on matters related to high-risk travellers. This team provides members to the NS-JOC, which produces analyses on emerging high-risk traveller trends, contributes to the identification of high-risk travellers, and coordinates CBSA's national response to high-risk traveller lookouts and investigations. CBSA's High-Risk Traveller team also reviews disclosures of high-risk traveller personal information to ensure that the information was lawfully obtained and disclosed.[196] In 2017, CBSA reviewed all of the cases investigated by NS-JOC in 2016 and found that the high-risk traveller initiative played a direct role in denying *** individuals access to Canada. Table 31 illustrates CBSA's participation in the NS-JOC specifically relating to high-risk travellers.

NS-JOC High-Risk Traveller Results Measure	2014	2015	2016	2017	2018
Investigative leads received from partners	***	***	***	***	***
Investigative leads generated for partners	***	***	***	***	***
Issued national security lookouts	***	***	***	***	***

Source: CBSA, Written response to NSICOP Secretariat questions: Question 2, July 5, 2019.

Table 31: CBSA National Security Joint Operations Centre (NS-JOC) High-Risk Traveller Results Measures 2014–2018

[196] CBSA, Flash Note to the Director: Information Disclosure of Personal Information for Associates/Family, Briefing note, March 22, 2017.

Governance of national security and intelligence activities

Ministerial direction

431. This section describes the mechanisms CBSA has put in place to govern its national security and intelligence activities.

432. The Minister has provided CBSA with two ministerial directions for its national security and intelligence activities:[197]

- **Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities** (2017) states the government's commitment to values and principles against torture and mistreatment. It prohibits the disclosure of information that would result in a substantial risk of mistreatment of an individual by a foreign entity, the making of requests for 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.[198]
- **The Ministerial Direction on Intelligence Priorities** (2017) guides the implementation of the government's intelligence priorities, and is meant to support ministerial accountability for CBSA's administration and enforcement of its program legislation.

433. The Ministerial Direction on Intelligence Priorities identified the following principles to guide and inform all CBSA activities in support of the intelligence priorities:

- CBSA's program legislation and the *Canadian Charter of Rights and Freedoms* shall be respected;
- the privacy of individuals shall not be infringed on unless and only to the extent that there are valid reasons to do so;
- CBSA shall ensure adequate and consistent handling of personal information when collecting, storing, sharing and disclosing information in accordance with privacy legislation and government information classification policies and standards; and
- information sharing with foreign partners shall respect the Ministerial Direction to CBSA: Information Sharing with Foreign Partners (which was later replaced by the Ministerial Direction to CBSA: Avoiding Complicity in Mistreatment by Foreign Entities).

---

[197] In 2017, CBSA received ministerial direction on minors in Canada's immigration system. This direction is not directly related to national security and intelligence, and will only be referred to for comparative purposes.

[198] Minister of Public Safety and Emergency Preparedness, *Ministerial Direction to the Canada Border Services Agency: Avoiding Complicity in Mistreatment by Foreign Entities*, www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/msnstrl-drctn-cbsa-asfc-en.aspx.

434. The Ministerial Direction on Intelligence Priorities contains one reference to the accountability of CBSA to the Minister.

> In the course of implementing these intelligence priorities, CBSA shall immediately inform [the Minister] when there is a potential that a CBSA activity may have a significant adverse impact, such as posing a risk to human life; discrediting CBSA or the Government of Canada; negatively affecting Canadian relations with any country or international organization of state; and/or, contravening any of the guidelines set out in this directive.[199]

435. Since the issuance of the ministerial direction, CBSA has informed the Minister of Public Safety and Emergency Preparedness of one instance where a CBSA activity met this obligation. In that case, the President of CBSA described the granting of permanent resident status to a foreign national of national security concern in August of 2017 [***The rest of this sentence and the next were revised to remove injurious or privileged information. The sentences describe the potential implications. ***][200] The Committee examined this case in detail and notes that CBSA and IRCC have put in place measures to prevent similar cases in the future.

436. Outside of the accountability obligation noted above, the Ministerial Direction on Intelligence Priorities for 2017–2019 contains no requirement for regular reporting (e.g., annual reporting) to the Minister on CBSA's national security or intelligence activities. This is in contrast to other ministerial directions provided to CBSA, which include obligations for regular reporting on activities.[201]

437. CBSA has not received ministerial direction on any of its more sensitive activities, such as the use of surveillance or confidential human sources, ***[202]

438. The Committee is aware that CBSA had drafted a proposed ministerial direction on two of its sensitive national security and intelligence activities, surveillance and confidential human sources. The draft Ministerial Direction proposed a number of limitations and requirements for the conduct of these activities, and set out specific reporting requirements to the Minister.[203] Ultimately, the Minister of Public Safety and Emergency Preparedness did not provide such direction.

---

[199] Minister of Public Safety and Emergency Preparedness, *Ministerial Direction to the Canada Border Services Agency: Intelligence Priorities for 2017–2019*, undated.

[200] CBSA President, Subject of National Security Concern Granted Permanent Residency. For the Minister, Briefing note. September 29, 2017.

[201] These include, for example, a quarterly report in regards to the detention and housing of minors, and an annual report to the Minister in regards to avoiding complicity in mistreatment by foreign entities.

[202] ***

[203] CBSA, *Update on MD to CBSA for Surveillance and CHS*, April 9, 2014.

Internal governance of national security and intelligence activities

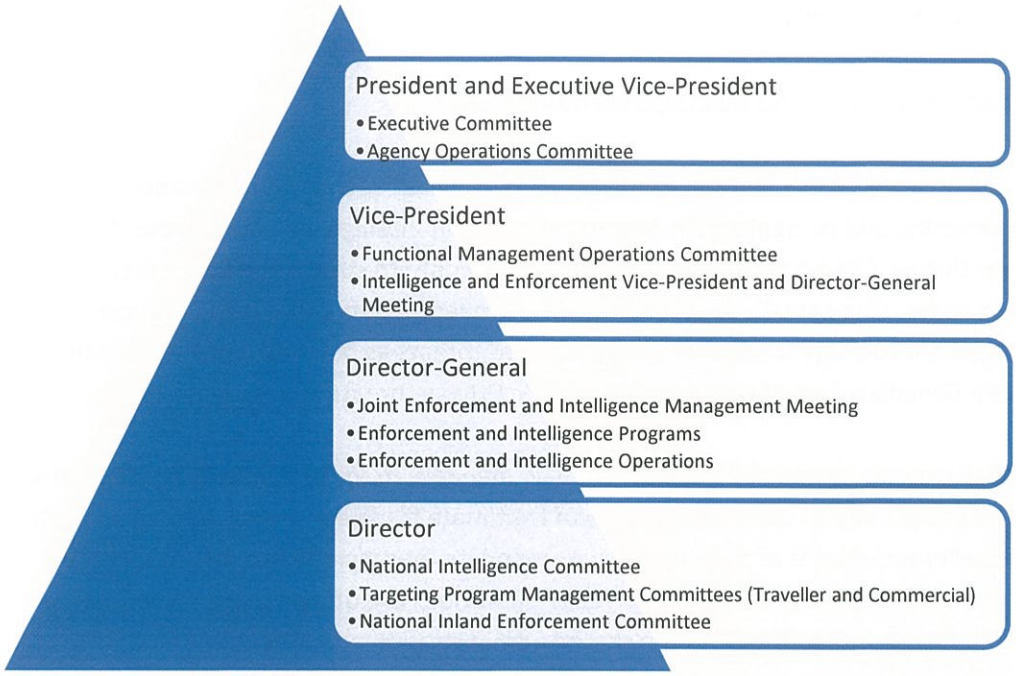
439. CBSA's management of its national security and intelligence activities falls within its broader governance structures. In April 2019, CBSA replaced its previous model of governance of distinct Programs and Operations streams with a new Functional Management model. The new model blends previous areas of programs, policy and operations into three new branches: Travellers, Commercial and Trade, and Intelligence and Enforcement.[204] Each branch is led by a vice-president who is accountable for program development, design and delivery. The vice-presidents will establish program priorities and provide national direction to the regions. As part of this shift, CBSA also created a Chief Transformation Officer and established a new Strategic Policy Branch.[205]

440. CBSA stated that the shift to a new governance model had three objectives. First, the blending of CBSA's Programs and Operations branches is meant to provide clarity within the organization pertaining to roles and responsibilities, consistent with internal assessments that found that the previous division between Programs and Operations resulted in confusion over the precise roles, responsibilities and accountabilities of front-line practitioners and senior management.[206] Second, by reorganizing the branches under designated vice-presidents as leads, the model is designed to create clearer lines of accountability and responsibility. Third, CBSA sought to improve efficiency, both financially and in facilitating the movement of low-risk goods and persons.[207] CBSA stated that "[t]hese organizational changes will improve the Agency's ability to make the critical, results-based decisions that keep Canadians safe and prosperous."[208]

441. As part of its governance structure, CBSA established a number of bodies to provide guidance on pertinent issues, and to elevate problems to senior decision-making bodies where required. CBSA's governance structure for its Intelligence and Enforcement Program comprises four levels, as shown in Figure 1.

---

[204] CBSA, CBSA 2004–2019, Presentation to NSICOP Secretariat, March 1, 2019.
[205] CBSA, NSICOP hearing, May 7, 2019.
[206] CBSA, Comments from the CBSA President, NSICOP hearing, May 7, 2019. See also: CBSA, *Review of the Confidential Human Source (CHS) Program*, July 2014.
[207] CBSA, Comments from the CBSA President, NSICOP hearing, May 7, 2019.
[208] CBSA, Canada Border Services Agency Quarterly Financial Report For the quarter ended June 30, 2018, August 29, 2018, www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/fs-ef/2018/qfr-rft-q1-eng.html.



Source: CBSA, "Review of CBSA National Security and Intelligence Activities," Presentation to NSICOP, May 7, 2019.

Figure 1: CBSA's governance structure for its Intelligence and Enforcement Program

442. CBSA officials also attend multiagency committees on national security and intelligence. To maintain interdepartmental coordination on operations, the CBSA President attends the weekly Deputy Ministers' Operations Committee, chaired by the Privy Council Office with representation from the security and intelligence community. CBSA vice-presidents attend interdepartmental assistant deputy minister (ADM) meetings, including the National Security Operations Committee and the National Security Policy Committee. To maintain interdepartmental coordination on policy and administration, CBSA's President is a member of the deputy ministers' committees on National Security and on Intelligence Assessment, and separate committees on Global Trends and Foreign Affairs and Defence, all which convene monthly. CBSA's vice-presidents participate in a number of ADM-level multiagency fora, including ADM committees on national security policy, intelligence, intelligence assessment, and money laundering and terrorism financing. CBSA directors-general, directors and managers also participate in a variety of issue-specific committees across the government.

The Committee's Assessment

CBSA's role in Canada's security and intelligence community

444. The Committee accepts CBSA's statement that it plays a "niche" role within the national security and intelligence community, and recognizes the important role that intelligence plays across the full spectrum of CBSA's activities. CBSA has no specific statutory mandate to conduct national security and intelligence activities; rather it does so in support of its program legislation. CBSA uses intelligence to develop a risk management strategy to identify border-related threats as far in advance as possible before they arrive at a Canadian port of entry, and to interdict these threats and mitigate them.

445. CBSA's national security responsibilities flow from its mandate to make admissibility decisions concerning goods and people and to facilitate the flow of legitimate trade and travel. CBSA's conduct of sensitive national security activities is of clear value to its mandate, particularly its work in security screening, immigration enforcement and targeting. Those operations are of significant value to other government departments too, notably IRCC in the shared administration and enforcement of IRPA, and CSIS in the identification of unknown threats to the security of Canada.

Ministerial direction and national security and intelligence activities

446. Since 2013, [*** The following sentence was revised to remove injurious or privileged information. The sentence notes that the department was aware that its sensitive intelligence-gathering activities, including the use of surveillance and confidential human sources, would benefit from ministerial direction.[209] ***]The Committee believes ministerial direction would clarify CBSA's mandate, authorities and accountability obligations for sensitive activity areas, and would bring CBSA in line with its partners, who have received ministerial direction in these areas.

447. As is the case with ministerial direction to CBSA on implementing the government's intelligence priorities, direction is important both for ministerial accountability and to help CBSA prioritize its resources. CBSA's own tiered system of enforcement and intelligence priorities is aligned with its risk-based approach to border management and border enforcement, and helps CBSA dedicate its resources to areas of highest risk.

National security and intelligence partnerships

448. CBSA's partnerships improve the efficacy of its operations while contributing to the effective operations of the wider national security and intelligence community. Partnerships help CBSA to support national security and public safety priorities, and to achieve positive national security outcomes.

---

209 ***

Governance of national security and intelligence activities

449. CBSA's sensitive national security and intelligence activities are well governed. In each area, CBSA has implemented formal guidance, policy and standard operating procedures. Individual program areas and activities are subject to risk assessment and mitigation, internal audit and evaluation, and are expected to report internally to CBSA senior management on their activities. That said, internal CBSA reporting on its sensitive national security and intelligence activities is piecemeal and lacks a cumulative assessment of risks and outcomes. Consistency and clarity in annual reporting on CBSA national security and intelligence activities would improve CBSA's governance of its sensitive national security and intelligence activities.

450. CBSA's change to a new functional management structure is likely to strengthen its governance of sensitive national security and intelligence activities. At present, however, it is too early to make any definitive assessment on the outcomes of this change.

Conclusion

451. This review sought to understand CBSA's national security and intelligence activities in the context of its broader mandate and authorities. It then focused on three key areas: CBSA's conduct of sensitive national security and intelligence activities; its governance over those activities; and its relations with key Canadian partners in the areas of national security and intelligence.

452. CBSA has a large and complex mandate and significant responsibilities related to Canada's prosperity and security. Only a fraction of its work is evident to the majority of Canadians, whose engagement with CBSA is mostly limited to transactional exchanges at Canada's points of entry. Less evident is the range of security and intelligence activities that CBSA uses to facilitate the passage of low-risk people and goods and to identify and stop those of higher risk. Essential for enforcing CBSA's border-related mandate, those same activities make significant contributions to Canada's broader national security priorities. They are also the most sensitive activities conducted by the organization, owing to the risks they may pose to the rights and freedoms of Canadians.

453. Overall, the Committee is satisfied with CBSA's work in these areas. CBSA does not have an explicit legislative authority to investigate national security or organized crime, but it does have clear authority to conduct sensitive national security and intelligence activities that support its border-related responsibilities, consistent with the CBSA Act, the *Customs Act*, IRPA, the *Interpretation Act* and common law powers. These activities are managed through clear governance structures and a good understanding of their inherent risks. CBSA's work with other organizations in the security and intelligence community is similarly focused on enforcing its border-related mandate, and supports the work of those organizations where there is a clear link among their various mandates. Those relationships are based on clear governance structures and defined roles and responsibilities. Nevertheless, every system may be improved. The Committee makes six findings and two recommendations that it believes will strengthen the governance and accountability of CBSA national security and intelligence activities.

454. The Committee notes that CBSA set a high standard for engagement with the Committee. Its responses to Committee requests were consistently comprehensive and timely. It repeatedly made officials available to answer questions, provided practical demonstrations of activities conducted by the organization, and briefed the Committee alone and with its closest partners.

Findings

455. The Committee makes the following findings:

F14. While the Canada Border Services Agency (CBSA) does not have explicit legislative authority to investigate national security issues or organized crime, it is a core member of the national security and intelligence community, given its responsibility for border security. (Paragraph 334)

F15. Making admissibility determinations is the raison d'être of CBSA. CBSA uses national security and intelligence activities to identify whether goods and persons entering Canada are inadmissible. This can take place anywhere in Canada and, in some circumstances, overseas. CBSA works closely with its partners to execute its mandate for admissibility, most notably with Immigration, Refugees and Citizenship Canada on immigration security screening. (Paragraphs 305, 334–335 and 445)

F16. Intelligence and national security play different roles within CBSA's range of activities. Intelligence informs decision-making across the full range of CBSA decision-making and operations. On the other hand, CBSA has only a niche role in relation to national security, and its activities are directed at supporting national security *outcomes* within CBSA's broader customs and immigration mandate. (Paragraphs 305, 334 and 444-445)

F17. CBSA's authorities for engaging in national security and intelligence activities are clear. The *Canada Border Services Agency Act* establishes CBSA's mandate to support national security and public safety priorities and enforce its program legislation. CBSA's authority to control the importation and exportation of goods and make admissibility decisions is explicit in the *Customs Act* and the *Immigration and Refugee Protection Act* respectively. CBSA's use of particular national security and intelligence activities is implicitly derived from its enforcement mandate based on common law principles codified in the *Interpretation Act*. (Paragraphs 324–333)

F18. CBSA's sensitive national security and intelligence activities are well governed. However, CBSA does not have ministerial direction for its conduct of sensitive national security and intelligence activities. This is inconsistent with other organizations in the security and intelligence community that conduct similar activities and is a gap in ministerial accountability. (Paragraphs 437–438)

F19. In support of its mandate, CBSA conducts sensitive national security and intelligence activities that may pose a range of risks, including to the rights of individuals. While these activities are subject to governance controls, dedicated policy and operational guidance, CBSA does not have a standard process for assessing and reporting on the risks and outcomes of these national security and intelligence activities. (Paragraphs 436 and 449)

Recommendations

456. The Committee makes the following recommendations:

R7.	The Minister of Public Safety and Emergency Preparedness provide written direction to the Canada Border Services Agency on the conduct of sensitive national security and intelligence activities. That direction should include clear accountability expectations and annual reporting obligations.
R8.	The Canada Border Services Agency establish a consistent process for assessing and reporting on the risks and outcomes of its sensitive national security and intelligence activities.

Annex A: List of Findings

Chapter 1: Diversity and Inclusion in the Security and Intelligence Community

F1. In successive ministerial mandate letters and in its call to create a Security and Intelligence Diversity and Inclusion Tiger Team, the government identified the promotion and enhancement of diversity and inclusion as a priority in the security and intelligence community. This community approach has significant merit, but its implementation has fallen short. (Paragraphs 22, 68 and 69)

F2. Organizations in the security and intelligence community have put in place measures and programs to support employment equity, diversity and inclusion. However, the degree to which those organizations are diverse and inclusive differs significantly. (Paragraphs 36–50)

F3. In the past three years, the CAF and the RCMP settled lawsuits variously alleging widespread harassment, violence and discrimination. Progress on resolving and eradicating these underlying problems has been slow. CSIS also settled a lawsuit in 2017 specifically alleging Islamophobia, racism and homophobia in its Toronto Region office, and responded with an organization-wide Workplace Action Plan that same year. (Paragraphs 88–91)

F4. All of the organizations in the security and intelligence community have developed policies, training and awareness campaigns to combat and resolve harassment and violence in the workplace. However, some challenges exist with regard to survey analysis and tracking. This includes tracking harassment complaints, which can limit an organization's awareness of its prevalence. The issue of discrimination receives significantly less attention than harassment throughout the community. (Paragraphs 93–97)

F5. The representation of designated groups is lower than the public service average in a majority of the organizations under review. In a majority of the organizations under review, persons with disabilities are underrepresented overall and women are underrepresented at executive levels. Members of visible minorities are underrepresented both overall and at executive levels, and recruitment of members of visible minorities has stalled or decreased in several of the organizations under review over the past three years. There is currently not enough information available to assess the representation of Aboriginal peoples at executive levels across organizations under review. (Paragraphs 52–54)

F6. Inconsistencies in planning, monitoring and review undermine efforts to assess progress on diversity across the security and intelligence community. (Paragraphs 25–31)

F7. Accountability for diversity and inclusion across the security and intelligence community is insufficient. Organizations have not developed performance measurement frameworks, nor have they established measurable performance objectives for diversity and inclusion for executives or managers. Responsibility for advancing diversity and inclusion is not shared throughout most organizations, but is most often considered the sole responsibility of human

resources divisions. Weaknesses in the areas of accountability and responsibility undermine organizational efforts to advance organization-wide objectives. (Paragraphs 66–71)

Chapter 2: The Government Response to Foreign Interference

F8. Some foreign states conduct sophisticated and pervasive foreign interference activities against Canada. Those activities pose a significant risk to national security, principally by undermining Canada's fundamental institutions and eroding the rights and freedoms of Canadians. (Paragraphs 136–175)

F9. CSIS has consistently conducted investigations and provided advice to government on foreign interference. (Paragraphs 195–201)

F10. Throughout the period under review, the interdepartmental coordination and collaboration on foreign interference was case-specific and ad hoc. Canada's ability to address foreign interference is limited by the absence of a holistic approach to consider relevant risks, appropriate tools and possible implications of responses to state behaviours. (Paragraphs 219–227 and 280–285)

F11. Foreign interference has received historically less attention in Canada than other national security threats. This is beginning to change with the government's nascent focus on "hostile state activities." Nonetheless, the security and intelligence community's approach to addressing the threat is still marked by a number of conditions:

- There are significant differences in how individual security and intelligence organizations interpret the gravity and prevalence of the threat, and prioritize their resources. (Paragraphs 276–279)
- In determining the measures the government may use to address instances of foreign interference, responses address specific activities and not patterns of behaviour. Furthermore, the government's approach gives greater weight to short-term interests (e.g., foreign policy) than longer-term considerations (e.g., risks to freedoms, rights and sovereignty). (Paragraphs 281–285)

F12. Government engagement on foreign interference has been limited.

- With the exception of CSIS outreach activities, the government's interaction with sub-national levels of government and civil society on foreign interference is minimal. (Paragraphs 256–267)
- Engagement is limited in part by the lack of security-cleared individuals at the sub-national level. (Paragraph 261)
- There is no public foreign interference strategy or public report similar to those developed for terrorism or cyber security. (Paragraphs 289–291)

F13. Canada is working increasingly with its closest allies and partners to address foreign interference. This is essential for Canada. (Paragraphs 268–274)

Chapter 3: The Canada Border Services Agency's National Security and Intelligence Activities

F14. While the Canada Border Services Agency (CBSA) does not have explicit legislative authority to investigate national security issues or organized crime, it is a core member of the national security and intelligence community, given its responsibility for border security (Paragraph 334).

F15. Making admissibility determinations is the raison d'être of CBSA. CBSA uses national security and intelligence activities to identify whether goods and persons entering Canada are inadmissible. This can take place anywhere in Canada and, in some circumstances, overseas. CBSA works closely with its partners to execute its mandate for admissibility, most notably with Immigration, Refugees and Citizenship Canada on immigration security screening (Paragraphs 305, 334–335 and 445).

F16. Intelligence and national security play different roles within CBSA's range of activities. Intelligence informs decision-making across the full range of CBSA decision-making and operations. On the other hand, CBSA has only a niche role in relation to national security, and its activities are directed at supporting national security outcomes within CBSA's broader customs and immigration mandate (Paragraphs 305, 334 and 444-445).

F17. CBSA's authorities for engaging in national security and intelligence activities are clear. The Canada Border Services Agency Act establishes CBSA's mandate to support national security and public safety priorities and enforce its program legislation. CBSA's authority to control the importation and exportation of goods and make admissibility decisions is explicit in the Customs Act and the Immigration and Refugee Protection Act respectively. CBSA's use of particular national security and intelligence activities is implicitly derived from its enforcement mandate based on common law principles codified in the Interpretation Act (Paragraphs 324–333).

F18. CBSA's sensitive national security and intelligence activities are well governed. However, CBSA does not have ministerial direction for its conduct of sensitive national security and intelligence activities. This is inconsistent with other organizations in the security and intelligence community that conduct similar activities and is a gap in ministerial accountability (Paragraphs 437–438).

F19. In support of its mandate, CBSA conducts sensitive national security and intelligence activities that may pose a range of risks, including to the rights of individuals. While these activities are subject to governance controls, dedicated policy and operational guidance, CBSA does not have a standard process for assessing and reporting on the risks and outcomes of these national security and intelligence activities (Paragraphs 436 and 449).

Annex B: List of Recommendations

Chapter 1: Diversity and Inclusion in the Security and Intelligence Community

R1. The Committee conduct a retrospective review in three to five years to assess the security and intelligence community's progress in achieving and implementing its diversity goals and inclusion initiatives, and to examine more closely the question of inclusion, including issues of harassment, violence and discrimination, through closer engagement with employees.

R2. The security and intelligence community adopt a consistent and transparent approach to planning and monitoring of employment equity and diversity goals, and conduct regular reviews of their employment policies and practices (that is, employment systems reviews) to identify possible employment barriers for women, Aboriginal peoples, members of visible minorities and persons with disabilities.

R3. The security and intelligence community improve the robustness of its data collection and analysis, including GBA+ assessments of internal staffing and promotion policies and clustering analyses of the workforce. In this light, the Committee also highlights the future obligation for organizations to investigate, record and report on all occurrences of harassment and violence in the workplace.

R4. The security and intelligence community develop a common performance measurement framework, and strengthen accountability for diversity and inclusion through meaningful and measurable performance indicators for executives and managers across all organizations.

Chapter 2: The Government Response to Foreign Interference

R5. The Government of Canada develop a comprehensive strategy to counter foreign interference and build institutional and public resiliency. Drawing from the Committee's review and findings, such a strategy should:

a. identify the short- and long-term risks and harms to Canadian institutions and rights and freedoms posed by the threat of foreign interference;

b. examine and address the full range of institutional vulnerabilities targeted by hostile foreign states, including areas expressly omitted in the Committee's review;

c. assess the adequacy of existing legislation that deals with foreign interference, such as the Security of Information Act or the Canadian Security Intelligence Service Act, and make proposals for changes if required;

d. develop practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states;

e. establish regular mechanisms to work with sub-national levels of government and law enforcement organizations, including to provide necessary security clearances;

f. include an approach for ministers and senior officials to engage with fundamental institutions and the public; and

g. guide cooperation with allies on foreign interference.

R6. The Government of Canada support this comprehensive strategy through sustained central leadership and coordination. As an example of a centralized coordinating entity to address foreign interference, the Committee refers to the appointment and mandate of the Australian National Counter Foreign Interference Coordinator.

The Committee reiterates its recommendation from its Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018:

> In the interest of national security, members of the House of Commons and Senate should be briefed upon being sworn-in and regularly thereafter on the risks of foreign interference and extremism in Canada. In addition, Cabinet Ministers should be reminded of the expectations described in the Government's Open and Accountable Government, including that Ministers exercise discretion with whom they meet or associate, and clearly distinguish between official and private media messaging, and be reminded that, consistent with the Conflict of Interest Act, public office holders must always place the public interest before private interests.

Chapter 3: The Canada Border Services Agency's National Security and Intelligence Activities

R7. The Minister of Public Safety and Emergency Preparedness provide written direction to the Canada Border Services Agency on the conduct of sensitive national security and intelligence activities. That direction should include clear accountability expectations and annual reporting obligations.

R8. The Canada Border Services Agency establish a consistent process for assessing and reporting on the risks and outcomes of its sensitive national security and intelligence activities.

Annex C: Committee Outreach and Engagement

Committee Meetings and Hearings:

Canada Border Services Agency

- President
- Vice President, Strategic Policy Branch
- Director, Intelligence, Targeting and Criminal Investigations Program Management
- Executive Director and Senior Executive Counsel
- Acting Executive Director, External Review

Canadian Security Intelligence Service

- Director
- Deputy Director, Operations
- Assistant Director, Intelligence
- Assistant Director, Policy
- Director General, Counter-Intelligence and Counter-Proliferation
- Director General, Intelligence Assessment
- Director General, Ottawa Region
- Director General, Security Screening Branch
- Deputy Director General, Counter-Intelligence and Counter-Proliferation
- Acting Director General, External Review and Compliance
- Head, Intelligence Assessments Branch

Global Affairs Canada

- Deputy Minister
- Assistant Deputy Minister, International Security and Political Affairs
- Director General, Counter-Terrorism, Crime and Intelligence
- Director General, Human Rights, Freedom and Inclusion
- Executive Director, Threat Assessment and Intelligence Services

Immigration, Refugees and Citizenship Canada

- Director General, Case Management Branch
- Senior Director, International Network

Justice Canada

- Deputy Assistant Deputy Attorney General, National Litigation Sector
- Director and General Counsel, National Security Group

Privy Council Office

- National Security and Intelligence Advisor to the Prime Minister
- Assistant Secretary to Cabinet, Security and Intelligence

- Assistant Secretary to Cabinet, Intelligence Assessment
- Director of Strategic Policy and Planning, Security and Intelligence
- Senior Policy Analyst, Strategic Policy and Planning, Security and Intelligence

Royal Canadian Mounted Police

- Deputy Commissioner, Federal Policing
- Assistant Commissioner, Federal Policing Criminal Operations
- Assistant Commissioner, Intelligence and International Policing
- Executive Director, National Security
- Officer in Charge, National Security Joint Operations Centre
- Policy Analyst, Federal Policing Strategic Direction

Academics and former officials

- Mel Cappe
- David Mulroney
- Luc Portelance

Annex D: Glossary

ADM	Assistant deputy minister
API	Advance Passenger Information
Border Five (B5)	Allied federal agencies tasked with border security in the allied nations of Canada, the United Stated, the United Kingdom, Australia and New Zealand
CACP	Canadian Association of Chiefs of Police
CBSA	Canada Border Services Agency
CCP	Chinese Communist Party
CFINTCOM	Canadian Forces Intelligence Command
CHS	Confidential human source
CIC	Citizenship and Immigration Canada (see IRCC)
CM	Civilian Members of the RCMP
CRCC	Civilian Review and Complains Commission of the RCMP
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSSAs	Chinese Students and Scholars Associations
DND/CAF	Department of National Defence/Canadian Armed Forces
ESDC	Employment and Social Development Canada
FINTRAC	Financial Transactions and Reports Analysis Centre
Five Eyes	Allied nations of Canada, the United States, the United Kingdom, Australia and New Zealand
GAC	Global Affairs Canada
GBA+	Gender-based analysis plus
IBET	Integrated Border Enforcement Team
INSET	Integrated National Security Enforcement Team
IRCC	Immigration, Refugees and Citizenship Canada
IRPA	*Immigration and Refugee Protection Act*
ITAC	Integrated Terrorism Assessment Centre
LMA	Labour market availability

MP	Member of Parliament
MOU	Memorandum of understanding
MSOC	Marine Security Operations Centre
NS-JOC	National Security Joint Operations Centre
NSES	National Security Enforcement Section
NSIA	National Security and Intelligence Advisor to the Prime Minister
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
PCO	Privy Council Office
PNR	Passenger Name Record
PRC	People's Republic of China
PS	Public Safety Canada
PSE	Public service employees
PSES	Public Service Employment Survey
RCMP	Royal Canadian Mounted Police
RM	Regular Members of the RCMP
SCIDA	*Security of Canada Information Disclosure Act*
SIRC	Security Intelligence Review Committee
TBS	Treasury Board of Canada Secretariat
TRM	Threat reduction measure
TUSCAN	TIPOFF U.S.-Canada
WFA	Workforce availability