The National Security and Intelligence Committee of Parliamentarians

2022 Annual Report

Canada

The National Security and Intelligence Committee of Parliamentarians
Annual Report 2022 (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 2022 (Version révisée selon le paragraphe 21(5) de la Loi sur le CPSNR)

P.O. Box 8015, Station T, Ottawa ON K1G 5A6
www.nsicop-cpsnr.ca

Annual Report 2022

The National Security and Intelligence Committee of Parliamentarians

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 report was provided to the Prime Minister on May 12, 2023. No revisions were made to remove information the disclosure of which the Prime Minister believes would be injurious to national defence, national security or international relations, or which constitutes solicitor-client privilege.

However, the report's annexes of the Committee's previous recommendations and the government's responses do contain revisions that were included in previous reports. Each of these are marked with three asterixis (***). There are no changes to these revisions.

Chair's Message

I am pleased to submit the Committee's fifth annual report to the Prime Minister. In 2022, the Committee finished its review of the national security and intelligence activities of Global Affairs Canada, continued its review of the Federal Policing mandate of the Royal Canadian Mounted Police, and met with international partners, among other work.

As 2022 marked the fifth anniversary of the creation of the Committee and as Parliament is required to conduct a review of the *National Security and Intelligence Committee of Parliamentarians (NSICOP) Act* in 2023, this Annual Report begins with a retrospective on the Committee's work since 2017, discusses the key challenges it is facing today, and highlights themes for possible reform of the Act.

Consistent with the NSICOP Act, this report also provides a summary of the Committee's special report concerning Global Affairs Canada and fulfills other statutory reporting obligations.

Canadians expect their security agencies to be held accountable for their actions. This is why the government established the Committee.

Marking five years of the Committee

I am privileged to mark the five-year anniversary of the Committee, which began its work in December 2017. Canadians expect their national security and intelligence agencies to counter threats and keep us safe while respecting the law, and the rights and freedoms of all Canadians. We also expect them to be held accountable for their actions. This is why the government established the Committee. The Committee is Canada's first review body consisting entirely of parliamentarians, and the first review body that can review national security and intelligence activities across the government.

The *National Security and Intelligence Committee of Parliamentarians Act* came into force on October 6, 2017. The Committee was announced by the Prime Minister on November 6, 2017, held its first meeting in December 2017, and began site visits with agencies of the security and intelligence community in January 2018. Since then, there have been two elections, three iterations of the Committee (and three different meeting and office locations), and 27 new and continuing members.

In its first five years, the Committee completed nine reviews, and is currently working on three others. The Committee's reviews strengthened the security and intelligence community's policies and operations, as well as overall accountability. The reviews also shone a light on the important work of the community, and on the challenges the community faces in an uncertain world.

Opportunities and challenges

With all this in mind, our 2022 Annual Report begins by taking stock of the past five years and briefly surveys several issues and challenges. Two bear mentioning here.

First, the Committee believes that the government's decision to formally respond to the Committee's recommendations is essential to strengthening the policies, operations and accountability of the security and intelligence community. The government responded to the Committee's recommendations for the first time in 2021, and it did so again in response to the Committee's special report on the national security and intelligence activities of Global Affairs Canada, which was tabled in Parliament in November 2022. In our last annual report, we indicated that we would be seeking status updates from the government on all of the Committee's previous recommendations, in order to understand the impact of those recommendations and their implementation. However, as of December 31, 2022, the government has not responded to that request relating to the 22 recommendations made in the Committee's previous seven reviews. We continue to expect that such a response will be forthcoming.

Second, the Committee faces three challenges with obtaining the information it is entitled to by law and that it requires to fulfil its mandate. First, some departments have cited reasons outside the statutory exceptions found in the *National Security and Intelligence Committee of Parliamentarians Act* for not providing information that the Committee requested in past reviews. Second, some departments selectively refused to provide relevant information, such as a departmental study, despite the Committee's right of access under its enabling legislation. Third, the Committee is concerned that an overbroad legal definition of what constitutes a Cabinet confidence has had an impact on the Committee's reviews. If departments were required to inform the Committee of how many and which relevant documents are being withheld and on what basis, then it would help resolve these challenges.

Over the past five years, the Committee has established a constructive relationship with the security and intelligence community that has strengthened its ability to conduct reviews while not impeding its independence. The Committee is encouraged by the progress made by departments in response to previous challenges, and believes that the present challenges can be resolved.

Conclusion

It is an honour to be the inaugural Chair of a committee that has done much to strengthen government accountability. I wish to thank my colleagues on the Committee, past and present, for their active participation and many insights. The work we do supports the effectiveness and accountability of the Canadian security and intelligence community. I also wish to thank the government officials and academics who appeared before the Committee to share their knowledge and wisdom, and my colleagues in other review bodies, in particular in the United Kingdom, for their advice over the years. Finally, on behalf of my colleagues, I would like to extend my gratitude to the Committee's Secretariat, which has supported the Committee's work with its professionalism and expertise.

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

The National Security and Intelligence Committee of Parliamentarians

(Membership from the 44th Parliament)

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

Mr. Stéphane Bergeron, M.P.

Mr. Don Davies, M.P.

The Hon. Dennis Dawson, Senator (resigned September 9, 2022)

Ms. Iqra Khalid, M.P.

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

Ms. Patricia Lattanzio, M.P.

Mr. James Maloney, M.P.

Mr. Rob Morrison, M.P.

Mr. Alex Ruff, M.S.C., C.D., M.P.

The Hon. Vernon White, Senator (resigned October 2, 2022)

Table of Contents

Chair's Message i

Introduction 1

The Committee's first five years, 2017 to 2022 1

Strengthening the effectiveness and accountability of the security and intelligence community 1

Challenges to obtaining relevant information 2

Areas for statutory reform 4

The Committee's work in 2022 4

Reporting requirements for 2022 5

Review of Global Affairs Canada (GAC) 7

Annex A: GAC Review findings and recommendations 9

Annex B: Recommendations of prior reviews 13

Annex C: Abbreviations 23

Introduction

1. The National Security and Intelligence Committee of Parliamentarians (NSICOP, or the Committee) is pleased to present the Prime Minister with its 2022 Annual Report. The report is divided into two parts. First, the Committee reflects on its first five years. This part concludes with an overview of the Committee's current challenges with obtaining information, and considerations for reforming the NSICOP Act, which Parliament is expected to begin reviewing in 2023. Second, the Committee fulfills its annual reporting requirements under the NSICOP Act, including by summarizing its work in 2022 and providing an overview of the special report it completed in 2022, the Special Report on the National Security and Intelligence Activities of Global Affairs Canada (GAC), and the government's response to its recommendations.

The Committee's first five years, 2017 to 2022

Strengthening the effectiveness and accountability of the security and intelligence community

2. The Committee was created when the NSICOP Act came into force on October 6, 2017.[1] Like our closest allies, Canada created a committee of parliamentarians from all political parties and from both houses of Parliament, cleared to view top secret and other sensitive information, with a mandate to conduct wide-ranging reviews of national security and intelligence frameworks and activities across the government.

3. The Committee's legal mandate is to review:

   a. the legislative, regulatory, policy, administrative and financial framework for national security and intelligence ('framework reviews');

   b. any activity carried out by a department that relates to national security or intelligence ('activity reviews'); and

   c. any matter relating to national security or intelligence that a minister of the Crown refers to the Committee ('referral reviews').

4. First constituted in December 2017, the Committee began 2018 with site visits and briefings at each of the core national security and intelligence departments to learn about the threats to the security of Canada and the role each department plays in countering those threats. The Committee also met with the Office of the Privacy Commissioner of Canada, the Office of the Auditor General of Canada, the Intelligence Commissioner (IC) and the National Security and Intelligence Review Agency (NSIRA) upon their creation, academics, experts, and several civil liberties groups on the interplay between human rights and security.

In its first five years, the Committee completed nine reviews and made 29 recommendations to strengthen the effectiveness and accountability of the security and intelligence community.

[1] Governor-in-Council, "Order Fixing the Day on which this Order is made as the Day on which the Act Comes into Force," Canada Gazette, order came into effect October 6, 2017, and was published October 18, 2017.

5. Also in 2018, the Committee determined its criteria for determining which security or intelligence activities to review. For the Committee to consider any review, the activity must involve one of the core members of the security and intelligence community. For national security issues, the activity must also relate to threats wto the security of Canada as defined in the *Canadian Security Intelligence Service Act* or criminality of national scope and gravity. For intelligence issues, the activity must involve the use of clandestine, covert, or privileged sources or methods. The Committee also decided on a list of other factors it considers, including whether the organization or activity was previously subject to review, and whether there is a high level of public interest in the topic.[2]

6. The Committee believes that its nine reviews over the past five years have served three primary objectives. First, the Committee's 61 findings and 29 recommendations sought to strengthen the effectiveness and accountability of the many departments and agencies that make up the security and intelligence community. Second, the revised versions of the Committee's reports – which are tabled in Parliament and published to the Committee's website – improved transparency by informing parliamentarians and the public about the government's security and intelligence activities. Third, the Committee's reports and stakeholder engagement informed the democratic debate about national security and intelligence, and our rights and freedoms. The Committee is grateful to its colleagues on the House of Commons' Standing Committee on Public Safety and National Security and the Standing Senate Committee on National Security, Defence and Veterans Affairs, as well as the academic community, for their engagement with its reports.

7. One of the Committee's first reviews, which examined the government's process for setting intelligence priorities, exemplified all three of the Committee's primary objectives. The Committee's recommendations sought to improve the intelligence priority setting process, coordination, and reporting on results. The review was an act of transparency, as it provided Parliamentarians and Canadians with previously unpublished information about a process that involves all core members of the security and intelligence community. The review also bolstered accountability over an area of operations that is high-risk because of its sensitivity and potential impact on the rights of Canadians. This review is just one example of how a committee of security cleared parliamentarians strengthened the operations and accountability of a security and intelligence activity of strategic importance.[3]

Challenges to obtaining relevant information

8. The Committee has a broad mandate to enhance the accountability of the security and intelligence community. The Committee can only discharge its mandate if it has broad access to relevant information.

9. When the Committee was established, only the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP) were subject to review by independent review bodies.

---

[2] NSICOP, Annual Report 2018, 2019.
[3] NSICOP, "Reports," webpage.

Departments that were new to national security and intelligence review responded in different ways. Some immediately set a high standard for engagement with the Committee while others required more time to achieve an ability to provide the Committee with information that was comprehensive and timely.

The Committee has encountered problems obtaining government information that it is entitled to by law.

10. While some in the security and intelligence community may have been apprehensive about providing top secret information to a committee of parliamentarians, the Committee has always believed that it is in the best interests of the agencies to be frank and forthcoming with NSICOP. For its part, the Committee's approach has always been to build trust and maintain an open dialogue with the departments and agencies under review without compromising its independence. The Committee was encouraged when the National Security and Intelligence Advisor to the Prime Minister established a review liaison unit in PCO to coordinate the response to reviews and to coordinate review-related work across the government, and that most departments and agencies have now established liaison units to act as their central point of contact for NSICOP. Nonetheless, challenges remain.

11. According to the NSICOP Act, 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," with several narrow exceptions that are expressly stated in the Act. Over the past five years, however, the Committee has encountered problems obtaining the information that it is entitled to by law. First, several departments cited reasons outside the statutory exceptions as a rationale for not providing information, such as inappropriately claiming that relevant emails, draft policies or departmental studies should not be provided to the Committee.

12. Second, some departments selectively refused to provide information even though the information fell within a request for information from the Committee. In several cases, the Committee came across the information later or through other sources, such as subsequent media reporting based on information disclosed by those very departments under the *Access to Information Act.* This is an important problem, because the Committee is unaware of what information is being withheld, which could undermine its ability to fulfil its mandate.

13. Third, the Committee is concerned that departments are applying an overly broad interpretation of what constitutes a Cabinet confidence, one of four statutory limitations to the Committee's right of access to information. For example, during the review of the national security and intelligence activities of Global Affairs Canada (GAC), information that departments asserted was a Cabinet confidence turned out to have already been made public or to have simply been part of a briefing given to a Minister by their deputy head (but not policy advice to Cabinet or a committee of Cabinet). In each case, NSICOP argued that the assertion was inappropriate and, with one exception, the departments agreed. As the Committee wrote to the Prime Minister in June 2022, the core of the Committee's mandate is to improve Government accountability for national security and intelligence.[4] If departments continue to broadly interpret the definition of Cabinet confidence to withhold information and are not required to inform the Committee of what relevant information has been withheld and why, then the Committee's ability to transparently and comprehensively review the governance frameworks which support Ministerial accountability risks being compromised.

[4] NSICOP, Special Report on the National Security and Intelligence Activities of Global Affairs Canada, 2022.

Areas for statutory reform

14. Between 2017 and 2019, Parliament enacted legislation that created three new bodies with mandates to review national security and intelligence organizations or to provide oversight of certain activities: NSICOP, NSIRA and the IC, respectively. Consistent with provisions in the NSICOP Act and the *National Security Act, 2017,* the latter of which created NSIRA and the IC, Parliament is required to conduct "a comprehensive review of the provisions and operation" of both statutes.[5]

15. The Committee may make specific recommendations about reforming the NSICOP Act to the designated Parliamentary committee at the appropriate time. Here, it raises two broad themes for the government's consideration.

16. First, reforms to the NSICOP Act should improve the Committee's access to information and its ability to exchange information with other review bodies. In our reports, including this one, we have outlined some of the challenges the Committee has faced since its inception in obtaining information. The Act could be amended to address these issues. Second, the reforms of the NSICOP Act should enhance the independence and efficiency of the Committee. The Act could be amended to reflect the evolution of authorities of NSICOP's counterpart in the United Kingdom, the Intelligence and Security Committee.

17. The Committee looks forward to the resolution of the challenges it faces, informing Parliament's review of the NSICOP Act, receiving the government's responses to all its past and future recommendations, and continuing its review agenda.

The Committee's work in 2022

18. On January 20, 2022, following the 2021 federal election, the Prime Minister announced the re-appointment of the Honourable David McGuinty as the Chair of NSICOP, and the Committee's new and returning members for the 44th Parliament. On May 20, 2022, the Prime Minister announced the appointment of two new members to the Committee.

19. In 2022, the Prime Minister tabled the Committee's 2021 special report on the government's cyber defence framework. The Committee launched a review of the lawful interception of communications and the "going dark" challenge, completed its special report on the national security and intelligence activities of GAC, and continued its review of the Federal Policing mandate of the RCMP.

20. Between January 20 and December 31, 2022, the Committee met 25 times, 11 of which were hearings. It met with 41 officials from 12 federal organizations, either in-person or via secure video conference. It also held two briefings with a total of five academics.

[5] National Security and Intelligence Committee of Parliamentarians Act (S.C. 2017, c. 15), paragraph 34. National Security Act, 2017 (2019, c. 13), Part 9.

21. On February 14, 2022, the Prime Minister tabled the Committee's Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack. The report was submitted to the Prime Minister on August 11, 2021 and is summarized in the 2021 Annual Report. The government agreed with all four recommendations (Annex B).

22. On June 27, 2022, the Committee submitted its classified Special Report on the National Security and Intelligence Activities of Global Affairs Canada to the Prime Minister and the ministers of Foreign Affairs, National Defence, and Public Safety. On November 4, 2022, the Prime Minister tabled the revised version of the report in Parliament. The government agreed with all four recommendations. That special report is summarized in this annual report, and the Committee's recommendations, as well as the government's response, are contained in Annex A.

23. On August 18, 2022, the Committee announced the launch of its review of the lawful interception of communications by security and intelligence organizations and the "going dark" challenge. The Committee's review will examine the legislative, regulatory, policy and financial framework for the lawful interception of communications for security and intelligence activities, the challenges resulting from the impact of rapidly changing and emerging technology, including the use of end-to-end encryption, and any limitations of the current framework when faced with these challenges. NSICOP's review will also examine potential risks to the privacy rights of Canadians associated with modernizing authorities in this area.

24. Throughout 2022, the Committee held appearances and advanced its review of the RCMP's Federal Policing mandate, including numerous appearances and briefings by senior officials.

25. The Committee, as represented in most cases by its Chair, also met with international representatives from Australia, New Zealand and South Africa. The Chair also delivered presentations on the Committee and its work to the National Security Transparency Advisory Group and the Canadian Association for Security and Intelligence Studies, and met with the Director of the Canadian Institute for Cybersecurity and representatives of the United Nations Office on Drugs and Crime.

Reporting requirements for 2022

Injury to national security and refusal to provide information

26. The NSICOP Act has several reporting requirements. The Committee must include in its annual report the number of instances in the preceding year that an appropriate minister determined that a review conducted under paragraph 8(1)(b) of the Act would be injurious to national security. It must also 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 and would be injurious to national security, consistent with subsection 16(1) of the Act.

27. In 2022, no reviews proposed by the Committee were deemed injurious to national security by a minister and no information requested by the Committee was refused by a minister on those grounds.

Reviews deemed injurious to national security **0**
Information requests refused **0**

The Avoiding Complicity in Mistreatment by Foreign Entities Act

28. Pursuant to the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (the Act), twelve organizations within the federal government must submit to their Minister an annual report in respect of the implementation of the Act in the previous calendar year. The annual reports must contain information regarding:

- **a.** The disclosure of information to any foreign entity that would result in a substantial risk of mistreatment to an individual;
- **b.** The making of requests to any foreign entity for information that would result in a substantial risk of mistreatment of an individual; and
- **c.** The use of information that is likely to have been obtained through the mistreatment of an individual by a foreign entity.

29. The Act requires the implicated Ministers to provide a copy of their organization's annual mistreatment reports to NSICOP and NSIRA.

Avoiding Complicity in Mistreatment by Foreign Entities Annual Compliance Reports Received for 2021

The Committee received 2021 mistreatment reports from the following departments and agencies:

1. Canada Border Services Agency
2. Canada Revenue Agency
3. Canadian Security Intelligence Service
4. Communications Security Establishment
5. Department of National Defence and the Canadian Armed Forces
6. Financial Transactions and Reports Analysis Centre of Canada
7. Fisheries and Oceans Canada
8. Global Affairs Canada
9. Immigration, Refugees and Citizenship Canada
10. Public Safety Canada
11. Royal Canadian Mounted Police
12. Transport Canada

Referrals

30. Pursuant to paragraph 8(1)(c) of the NSICOP Act, any minister of the Crown may refer any matter relating to national security or intelligence to the Committee for review. The Committee did not receive any referrals in 2022.

Review of Global Affairs Canada (GAC)

31. On November 4, 2022, the Prime Minister tabled the Special Report on the National Security and Intelligence Activities of Global Affairs Canada (GAC, or the Department) in Parliament and the Committee published it to its website.[6] Consistent with its reporting obligations in the NSICOP Act, the Committee summarizes this review here.

The Committee was concerned by the near total absence of governance.

32. This review was the first in-depth examination of GAC's three broad national security and intelligence roles, which are to ensure foreign policy coherence, play a facilitation and advisory role for certain CSIS and CSE intelligence activities, and conduct its own security and intelligence activities. The Committee heard from senior officials from GAC, CSIS, and CSE, and focused on the Department's International Security and Political Affairs Branch.

33. The Department's broadest security and intelligence role is to ensure foreign policy coherence. This involves engaging CSIS, CSE and DND/CAF to ensure that they consider foreign policy interests when contemplating certain national security or intelligence activities. GAC has bilateral written arrangements with CSIS (2009), CSE (2009), and DND/CAF (2016). Its engagement with CSIS and CSE is formalized and involves longstanding joint oversight committees, but this is not the case for its engagement with DND/CAF. CSIS and CSE have policies and internal committees that govern how they consult GAC before collecting certain types of intelligence, conducting some operations, or concluding written arrangements with foreign security agencies.

34. The Committee identified significant weaknesses in the Department's *internal* governance of its foreign policy coherence role. The Department had no policies and few oversight committees, which may introduce weaknesses into the government's assessment of foreign policy risk. As for the Department's *external* governance, the formal nature of GAC's consultations with CSIS and CSE contrasts starkly with the nascent nature of its consultations with DND/CAF. The Committee recommended that the ministers of Foreign Affairs and National Defence put in place proactive, regular, and comprehensive consultation mechanisms to ensure that defence policies and operations are aligned with foreign policy objectives (Recommendation 1).

35. GAC produces and uses intelligence, funds international security projects, and coordinates the government's response to Canadians who are taken hostage abroad by terrorist groups. GAC is one of the largest consumers of intelligence in the federal government, which it uses primarily to safeguard embassies and consulates, and it collects intelligence around the world. The Committee was concerned by the absence of ministerial direction for these activities, and recommended that the Minister of Foreign Affairs provide written direction to the Department on its national security and intelligence activities (Recommendation 2).

[6] NSICOP, Special Report on the National Security and Intelligence Activities of Global Affairs Canada, 2022.

The most significant problem was political: successive governments failed to establish a framework to respond to terrorist hostage–takings abroad or provide direction on individual cases.

36. GAC plays an advisory and facilitator role in relation to certain CSIS and CSE operational activities. Although GAC has played a role in relation to CSIS's collection of foreign intelligence since the coming into force of the CSIS Act in 1984, unlike CSIS the Department has neither a policy nor a requirement to inform its minister about these activities. GAC and CSE cooperate in relation to CSE's foreign intelligence, cyber security, and cyber operations mandates. The coming into force of the CSE Act in August 2019 gave GAC a significant role in CSE's then new authorities to conduct cyber operations. The Act requires CSE to *consult* GAC before carrying out *defensive* cyber operations, and to obtain the *consent* of the Minister of Foreign Affairs before carrying out *active* cyber operations. While there is a GAC-CSE working group for these operations, CSE also has a ministerial direction that requires it to regularly report on the status and results of its cyber operations to its minister. GAC does not.

37. The Committee was also concerned by the near total absence of governance and formalized reporting to the minister regarding GAC's facilitator role. While GAC is not itself collecting this intelligence, addressing the potential impact of the exposure of the intelligence activities would fall to the Minister of Foreign Affairs, who must be kept informed so that they can provide direction and oversight. The Committee recommended that the Minister of Foreign Affairs put in place comprehensive governance mechanisms for the Department's security and intelligence activities and for those that it supports or contributes to at partner organizations (Recommendation 3).

38. One of GAC's key security activities is coordinating the government's response to terrorist hostage-takings and other international critical incidents. GAC has a three-person team that supports an interdepartmental task force, but in twenty years the Department has done little to prepare for these incidents: there is no policy framework, no training, and no routine tabletop simulation exercises for the task force. This undermines the Department's claim to "lead the coordination" of the government's response to international critical incidents, and tends to skew the government's response towards the mandate of the organization that brings the most capabilities to a particular incident. The Committee recommended that the Government of Canada establish a clear framework to respond to terrorist hostage-takings abroad (Recommendation 4).

39. In conclusion, the Committee's GAC review revealed a significant imbalance between the Department's significant role as a core member of the security and intelligence community and its governance mechanisms. Governance is the combination of internal and external structures and processes – including policies, procedures and oversight committees – that support prudent decision-making, accountability, and institutional memory. Governance serves accountability. Establishing a sound governance and accountability structure requires political will. The Committee came to five findings, and the government agreed with the Committee's four recommendations (Annex A).

Annex A: GAC Review findings and recommendations

Findings

F1. Global Affairs Canada (or the Department) is an integral part of the security and intelligence community. The Department advances Canada's national security interests abroad, provides critical support to its intelligence partners in the collection of foreign intelligence within Canada, and has an overarching role in ensuring the activities of its security and intelligence partners are coherent with the government's foreign policy interests and objectives.

F2. Global Affairs Canada ensures the foreign policy coherence of the security and intelligence community through a number of formal consultation mechanisms. The Department has established effective consultation mechanisms with the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE) to ensure the foreign policy coherence of their activities. Consultation between GAC and the Department of National Defence and the Canadian Armed Forces remains largely informal and ad hoc, and both organizations have been slow to respond to ministerial direction in this area.

F3. The internal governance of the Department's national security and intelligence activities is inconsistent, and in some areas completely absent. For its international security programs, the Department has strong governance mechanisms, including detailed policies, procedures and oversight committee structures. For its most sensitive intelligence activities, the opposite is true: the Department lacks policies, procedures or guidance documents, including for its role in requesting the collection of foreign intelligence within Canada *** or providing foreign policy risk assessments for CSIS and CSE activities.

F4. The absence of governance for the Department's most sensitive intelligence activities creates an important gap in ministerial accountability. The Department has no requirements to report regularly to the Minister of Foreign Affairs on the full spectrum of its national security and intelligence activities. This gap raises concerns about the Minister's awareness of the risk associated with the Department's most sensitive activities on an ongoing basis, and undermines the Minister's accountability for those activities.

F5. The Department's role in responding to terrorist hostage-takings abroad is neither leadership nor coordination, but facilitation and information sharing. At best, GAC convenes implicated departments with much greater operational roles and specific accountabilities, and works to build a coherent approach without authority to direct a whole-of-government response. Part of the challenge is one of the Department's own making: over the past 10 years, it has not developed the necessary policy, operational and training mechanisms for implicated government organizations to respond to such events coherently. Notwithstanding these gaps, the most significant problem is political: successive governments have failed to provide direction for a framework to address such critical incidents or provide specific direction on individual cases. Together, these challenges undermine the ability of the Department and its security and intelligence partners to respond effectively to terrorist hostage-takings.

Recommendations

R1. The Minister of Foreign Affairs work with the Minister of National Defence to put in place proactive, regular and comprehensive consultation mechanisms to ensure that Canada's defence policies and military operations are aligned with its foreign policy objectives.

R2. The Minister of Foreign Affairs provide written direction to the Department on its national security and intelligence activities. That direction should include clear accountability expectations and regular reporting requirements.

R3. The Minister of Foreign Affairs put in place comprehensive governance mechanisms for the Department's security and intelligence activities and for those that it supports or contributes to at partner organizations. Those mechanisms should better document processes and decision points to strengthen accountability and institutional memory.

R4. The Government of Canada establish a clear framework to respond to terrorist hostage takings, including to establish principles to guide the Government's response, identify triggers for Ministerial direction and engagement, establish leadership for whole of government responses to specific incidents, and provide sufficient resources to support operational requirements during critical incidents.

Status

The government agreed with the Committee's recommendations, and provided the following response.

GAC and DND's response to R1:

GAC and DND agree with this recommendation.

DND/CAF and GAC actively consult on many areas of defence policy and military operations. The ADM [Assistant Deputy Minister] Joint Consultative Mechanism (JCM), which meets regularly, is the primary, formal mechanism between the two organizations. GAC and DND/CAF are actively working together to enhance consultation mechanisms and will consider establishing additional mechanisms to address specific areas of operations, as appropriate. For example, GAC continues to work with DND/CAF to finalize a Memorandum of Understanding concerning consultations on defence intelligence activities, as well as an interdepartmental consultation process to ensure that CAF cyber operations are aligned with foreign policy objectives.

GAC's response to R2:

GAC agrees with and has acted upon this recommendation.

In 2022, the Minister issued a classified Ministerial direction to GAC on the nature and scope of the roles, responsibilities and activities of the Department's Intelligence Bureau. This document sets out regular reporting requirements for the Department's security and intelligence mandate outlining accountability expectations. Ministerial directions serve as a guidepost for the Department in fulfilling its national security and intelligence roles and responsibilities.

GAC response to R3:

GAC agrees with this recommendation.

In recent years, GAC has developed a number of governance mechanisms for the Department's security and intelligence activities. Notable examples are: the introduction of a Global Security Reporting Program Steering Committee, new governance instruments with the Canadian Security Intelligence Service, a framework for consultative engagement with the Communications Security Establishment on cyber operations, a draft interdepartmental engagement process with DND/CAF on cyber operations, and the negotiation of a Memorandum of Understanding with DND/CAF on consultations in relation to defence intelligence activities.

The introduction of these mechanisms has strengthened governance and accountability in regard to the Department's security and intelligence activities and for those that it supports or contributes to at partner organizations.

Joint PCO and GAC response to R4:

The government agrees with this recommendation.

The Government is committed to ensuring an effective whole of government response to international critical incidents (e.g. terrorist hostage-takings). Since the NSICOP review began, GAC has made significant progress on institutionalizing important foundational elements of the government's hostage recovery efforts. This included the establishment of a family policy and a family charter to provide clarity and transparency on how the government can provide support to victim's families.

A training program and table top exercises were conducted with officials from all relevant security and intelligence departments and agencies to promote understanding and operational coordination. Moving forward, this training will be held regularly to enhance the ability of the government to respond to international critical incidents.

In 2023, the government will work to clarify and strengthen the policy direction and response framework used to guide the management of terrorist hostage-takings. This will include GAC-led efforts to develop options in collaboration with departments and agencies to enhance and institutionalize the Government of Canada's hostage recovery activities. This will include, for example, potential improvements to family engagement practices, evaluating training needs, and assessing resource requirement to ensure an effective response to future critical incidents.

Annex B: Recommendations of prior reviews

Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018

Description

A special report on the allegations raised in the context of the Prime Minister's trip to India in February 2018 relating to foreign interference in Canadian political affairs, risks to the security of the Prime Minister, and the inappropriate use of intelligence.

Recommendations

Foreign interference

R1. In the interest of national security, members of the House of Commons and the 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. ***

R2. The Minister of Public Safety and Emergency Preparedness should consider revising the *** to include a formal role for the National Security and Intelligence Advisor. The information provided to the Committee demonstrates that the NSIA played a significant role ***. The Committee believes that the NSIA has a legitimate role to provide advice as coordinator of the security and intelligence community and advisor to the Prime Minister. ***

Security

R3. Drawing on the Committee's findings, an interdepartmental review should be undertaken to identify key lessons learned following these events.

R4. The Government should develop and implement a consistent method of conducting background checks by all organizations involved in the development of proposed guest lists for foreign events with the Prime Minister.

The use of intelligence

R5. The Prime Minister should review the role of the NSIA in the area of countering threats to the security of Canada. The Committee already made one recommendation with respect to the role of the NSIA in the area of ***. The Committee notes that a number of other government departments and agencies have statutory authority to take measures to protect Canada from threats to its security. The role of the NSIA should be clarified for those organizations, as well.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

Review of the Process for Setting Intelligence Priorities

Description

A review of the Government of Canada's process for establishing the national intelligence priorities, focusing on the governance of the process, the participation of the organizations involved, and performance measurement and resource expenditures.

Recommendations

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

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

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

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

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

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

Description

A review of the intelligence activities of the Department of National Defence and the Canadian Armed Forces. The Committee examined the scope of these activities, their legal authorities and the existing oversight mechanisms for their control and accountability.

Recommendations

R1. The Department of National Defence/Canadian Armed Forces (DND/CAF) review and strengthen its administrative framework governing defence intelligence activities, particularly with respect to the Ministerial Directive on Defence Intelligence, to ensure that it meets its own obligations on governance and reporting to the Minister of National Defence, and is properly tracking the implementation of those obligations. In particular:

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

R2. The Government amend Bill C-59, *National Security Act, 2017,* to ensure that the mandate of the proposed National Security and Intelligence Review Agency includes an explicit requirement for an annual report of DND/CAF activities related to national security or intelligence.

R3. Drawing from the Committee's assessment and findings, the Government give serious consideration to providing explicit legislative authority for the conduct of defence intelligence activities.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

However, the Mandate Letter sent to the Minister of Defence on December 13, 2019, included:

- "With the support of the Minister of Public Safety and Emergency Preparedness, introduce a new framework governing how Canada gathers, manages and uses defence intelligence, as recommended by the National Security and Intelligence Committee of Parliamentarians."[7]

The Committee recognizes that recommendation R2 was overtaken by events when Bill C-59, the *National Security Act, 2017* received Royal Assent on June 21, 2019, and did not include a requirement for NSIRA to produce an annual report of DND/CAF activities related to national security or intelligence.

[7] Prime Minister, "Minister of National Defence Mandate Letter," December 13, 2019.

Diversity and Inclusion in the Security and Intelligence Community

Description

A review that 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.

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.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these three recommendations (R2 to R4; R1 relates to the Committee).

The Government Response to Foreign Interference

Description

A review of the breadth and scope of foreign interference in Canada; the government's response; the implicated organizations and their response capabilities; the extent of coordination and collaboration among these organizations; the degree to which the government works with other levels of government and targets of foreign interference; and government engagement with allies abroad.

Recommendations

R1. 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:

- identify the short- and long-term risks and harms to Canadian institutions and rights and freedoms posed by the threat of foreign interference;
- examine and address the full range of institutional vulnerabilities targeted by hostile foreign states, including areas expressly omitted in the Committee's review;
- 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;
- develop practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states;
- establish regular mechanisms to work with sub-national levels of government and law enforcement organizations, including to provide necessary security clearances;
- include an approach for ministers and senior officials to engage with fundamental institutions and the public; and
- guide cooperation with allies on foreign interference.

R2. 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.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

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

Description

A review of the national security and intelligence activities of the Canada Border Services Agency, focusing on CBSA's governance over national security and intelligence activities in CBSA's Enforcement and Intelligence Program; CBSA's conduct of sensitive national security and intelligence activities; and CBSA's relations with its key partners in the areas of national security and intelligence.

Recommendations

R1. 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.

R2. 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.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

However, on February 16, 2022, the Minister of Public Safety issued the Ministerial Direction to the Canada Border Services Agency on Surveillance and Confidential Human Sources, which directs it to establish risk management and reporting mechanisms related to surveillance and confidential human sources.[8]

[8] Subsequently published to the web on June 15, 2022. Public Safety Canada, "Ministerial Directions," webpage, last modified August 29, 2022, accessed January 2023.

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 Defence Intelligence Activities

Description

A special report on the collection, use, retention and dissemination of information on Canadian citizens by the Department of National Defence and the Canadian Armed Forces in the conduct of defence intelligence activities, focusing on the operational context, legal framework, the CANCIT Function Directive, and the treatment of this information before the Directive.

Recommendations

R1. The Department of National Defence / Canadian Armed Forces (DND/CAF) rescind the Chief of Defence Intelligence Functional Directive: Guidance on the Collection of Canadian Citizen Information and, in consultation with the Privacy Commissioner, review all of its functional directives and other DND/CAF policy instruments that are relevant to the collection, use, retention and dissemination of information about Canadians to ensure consistent governance of these activities.

R2. To resolve the issue of the extraterritorial application of the Privacy Act, the Minister of National Defence should ensure DND/CAF complies with the letter and spirit of the Privacy Act in all of its defence intelligence activities, whether they are conducted in Canada or abroad.

R3. The Minister of National Defence introduce legislation governing DND/CAF defence intelligence activities, including the extent to which DND/CAF should be authorized to collect, use, retain and disseminate information about Canadians in the execution of its authorized missions.

Status

As of December 31, 2022, the government has not provided a status update regarding the implementation of these recommendations.

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

Description

A special report that describes the threat to government systems from malicious cyber actors; examines the evolution of the Government of Canada's cyber defence policies and laws; assesses the roles and responsibilities of relevant government organizations; and examines relevant case studies where government systems were compromised in cyber attacks.

Recommendations

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

R2. To the greatest extent possible, the government:

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

Status

The government provided the following responses to the recommendations made by the Committee:

Response to R1:

Agreed. Public Safety, Communications Security Establishment, and Treasury Board of Canada Secretariat agree that the government continue to strengthen its framework for defending government networks from cyber attack, ensuring that its authorities and programs for cyber defence are modernized as technology and other relevant factors evolve.

Public Safety, in collaboration with Communications Security Establishment and Treasury Board of Canada Secretariat, will continue to work together to align with the horizontal framework for cyber security to ensure that an appropriate governance structure is in place to advance cyber security policy.

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

Response to R2.1:

Agreed. The Treasury Board of Canada Secretariat will review the Treasury Board policy framework to ensure that cyber defence is applied equally to departments and agencies to the greatest extent possible. This includes alignment between the scope of the Policy on Government Security and the Policy on Service and Digital.

Responsible organization: Treasury Board of Canada Secretariat.

Response to R2.2:

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

Responsible organization: Treasury Board of Canada Secretariat.

Response to R2.3:

Agreed. Treasury Board of Canada Secretariat, in consultation with Shared Services Canada and Communications Security Establishment agree that the government should extend advanced cyber defence services, notably the Enterprise Internet Service of Shared Services Canada and the cyber defense sensors of the Communication Security Establishment, to all federal organizations to the greatest extent possible. Treasury Board of Canada Secretariat will continue to strengthen cyber defence measures as part of the updates to the Policy on Service and Digital, specifically through the mandatory procedures outlined under Appendix G: Standard on Enterprise IT Service Common Configurations of the Directive on Service and Digital which will be published in Early 2022.

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

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

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

Annex C: Abbreviations

CAF	Canadian Armed Forces
CSIS	Canadian Security Intelligence Service
CSE	Communications Security Establishment
DND	Department of National Defence
GAC, or the Department	Global Affairs Canada
IC	Intelligence Commissioner
NSICOP, or the Committee	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
RCMP	Royal Canadian Mounted Police