The National Security and Intelligence Committee of Parliamentarians

2021 Annual Report

Canada

The National Security and Intelligence Committee of Parliamentarians
Annual Report 2021 (Revised version pursuant to subsection 21(5) of the NSICOP Act)
CP100E-PDF (Online)
ISSN 2562-511X (Online)

Cette publication est également disponible en français :
Rapport annuel 2021 (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 2021

The National Security and Intelligence Committee of Parliamentarians

May 2022

Submitted to the Prime Minister on May 18, 2022

pursuant to subsection 21(1) of the National Security and Intelligence Committee of Parliamentarians Act

Revised version tabled in Parliament on September 28, 2022

pursuant to subsection 21(5) of the Act

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 18 May 2022. 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.

Chair's Message

Ottawa, ON – May 18, 2022

The past year continued to present significant challenges to the Committee and to all Canadians. For its part, the Committee continued to use the secure facilities of the security and intelligence community to fulfill its review mandate while respecting public health measures in place across Canada. This permitted us to finish one report, which we provided to the Prime Minister in August 2021, and lay the groundwork for two others, which are ongoing. The Committee was dissolved in August when the writs of election were issued, but the Committee's Secretariat continued the important work initiated by the Committee during its mandate.

Consistent with the *National Security and Intelligence Committee of Parliamentarians Act,* in this report the Committee provides a summary of the special report provided to the Prime Minister and fulfills its other reporting obligations.

The Committee believes that responses to its recommendations are essential to strengthening the operations and accountability of security and intelligence organizations.

Work of 2021

The Committee had a busy and productive year despite the public health challenges. Our Annual Report 2020 was tabled in Parliament in March 2021. That report contained a declassified summary of the major national security threats facing Canada. We also completed an in-depth review of Canada's cyber defences, which was provided to the Prime Minister in August 2021. A revised version was tabled in Parliament in February 2022. I encourage Canadians to read both reports.

The Committee also continued its work on two other reviews. The first is a review of the security and intelligence activities of Global Affairs Canada, for which the Committee has considered extensive documentation and held numerous appearances. It also launched a review of the federal policing activities of the Royal Canadian Mounted Police, and intends to hold relevant briefings and appearances for this review in the spring of 2022.

Opportunities and challenges

The coming year offers unique opportunities for the Committee and Parliament. In particular, Parliament is expected to begin a five year review of the NSICOP Act. This will mark an important milestone in the evolution of the Committee and an opportunity for Parliament to consider whether any changes to the Committee's enabling statute are necessary. We look forward to contributing to this discussion.

This year, the Committee was pleased to note the partial resolution of a long-standing challenge. For the first time, the government provided the Committee with a formal response to the recommendations included in one of its reports, the special report on government cyber defences. The Committee believes that responses to its recommendations are essential to strengthening the operations and accountability of security and intelligence

organizations. It welcomes the government's commitment, which it has cited as an area for improvement in past annual reports. It equally encourages the government to respond to the recommendations of the Committee's seven previous reviews of critical issues in the security and intelligence community, including the legal authority for the Department of National Defence and the Canadian Armed Forces to conduct its defence intelligence activities, and the absence of a whole of government strategy to address foreign interference in Canada. In the coming year, the Committee will engage with organizations implicated in the Committee's earlier reviews to determine whether they accept the Committee's recommendations and what actions have been taken to respond to them.

Conclusion

I would like to extend my sincere gratitude to my fellow committee members. The work we do supports the effectiveness of the Canadian security and intelligence community; your contributions are invaluable. I would also like to thank officials of the security and intelligence agencies for their cooperation during the review process. Finally, on behalf of my NSICOP colleagues, our thanks to the Secretariat for its unfailing support.

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 43rd Parliament)

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

Ms. Leona Alleslev, M.P.

Mr. Stéphane Bergeron, M.P.

Mr. Don Davies, M.P.

The Hon. Dennis Dawson, Senator

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

Mr. Peter Fragiskatos, M.P.

Ms. Iqra Khalid, M.P.

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

Mr. Rob Morrison, M.P.

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

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

Ms. Brenda Shanahan, M.P.

The Hon. Vernon White, Senator

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 fourth annual report. The report contains a summary of the comprehensive *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack,* a special review completed by the Committee in 2021, including the review's findings and recommendations. It also contains information on the Committee's work over the past year.

2. This year's Annual Report differs from past reports. In 2021, the Committee decided to provide its future reviews as special reports. This will disassociate the Committee's reviews from its annual reporting cycle, permitting the Committee to conduct complex reviews over varying timeframes and to provide its reports to the Prime Minister as soon as they are ready. As a result, the reports will be tabled in Parliament and available to Canadians in a timelier manner. Hereafter, the Committee's annual reports will focus more narrowly on the Committee's activities over the previous year and on fulfilling the reporting requirements identified in the *National Security and Intelligence Committee of Parliamentarians Act* (NSICOP Act).

The Committee's 2021 activities

3. Between January 1, 2021 and August 15, 2021, the Committee met ten times, four of which were hearings. It met with twenty-two officials from four different organizations, relying on a hybrid format of in-person meetings and secure video conferences.

4. In 2021, the Committee completed one framework review, under paragraph 8(1)(a) of the NSICOP Act, the *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack,* which included four findings and two recommendations. Two special reviews remain underway: Global Affairs Canada's security and intelligence activities and the Royal Canadian Mounted Police's Federal Policing mandate.

5. The Committee was dissolved in August 2021 when the writs of election were issued. The Committee's Secretariat continued to work on ongoing reviews, but no report could be finalized in the absence of a newly appointed Committee.

Reporting Requirements

Injury to National Security and Refusal to Provide Information

6. The NSICOP Act has a number of 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.

In 2021, 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.

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

Avoiding Complicity in Mistreatment by Foreign Entities

7. 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.

8. The Act requires the implicated Ministers to provide a copy of their organization's annual mistreatment reports to NSICOP and the National Security and Intelligence Review Agency (NSIRA).

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

In 2021, the Committee received reports from the following departments and agencies.

- Canada Border Services Agency
- Canada Revenue Agency
- Canadian Security Intelligence Service
- Communications Security Establishment
- Department of National Defence and the Canadian Armed Forces
- Financial Transactions and Reports Analysis Centre of Canada
- Fisheries and Oceans Canada
- Global Affairs Canada
- Immigration, Refugees and Citizenship Canada
- Public Safety Canada
- Royal Canadian Mounted Police
- Transport Canada

Referrals

9. On June 4, 2021, the Minister of Health sent a referral to the Committee pursuant to paragraph 8(1)(c) of the NSICOP Act regarding possible security incidents at the National Microbiology Laboratory in Winnipeg, Manitoba and the termination of two Canadian scientists. The Committee continues to consider the issue.

Summary of Cyber Defence Review

Government of Canada networks are a vital part of Canada's critical infrastructure.

10. On September 17, 2020, the Committee announced its review of the Government of Canada's framework and activities to defend its systems and networks from cyber attack. The classified version of the Committee's special report was delivered to the Prime Minister on August 11, 2021 and tabled in Parliament on February 14, 2022. This first-of-its-kind review 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.

11. As part of this review, the Committee examined documentation from the three organizations that play a leading role in developing and implementing the government's cyber defence framework: the Communications Security Establishment (CSE); Treasury Board of Canada Secretariat (TBS); and Shared Services Canada (SSC). The Committee received documentation covering the period from 2001 to 2021, principally to explore the evolution of the government's understanding of cyber threats and the authorities, governance mechanisms and activities needed to address them. The Committee held four hearings, two in 2020 and two in 2021. The Committee met with a total of 12 senior officials from CSE and TBS, and considered over 2,500 documents, representing over 37,000 pages of material.

12. The Committee made four findings (See Annex A). First, cyber threats to government systems and networks are a significant risk to national security and the continuity of government operations. Government of Canada networks are a vital part of Canada's critical infrastructure. The government uses them to collect and hold information, such as tax records, and to provide services, such as Employment Insurance, of fundamental importance to Canadians and Canadian businesses. The information they hold is also of significant value to Canada's adversaries, including state-sponsored cyber threat actors and cybercriminals.

13. Second, the government has built a robust, 'horizontal' cyber defence framework to defend its systems and networks from cyber attack. The evolution of this framework has been a mix of unanticipated and reactive, and deliberate and planned. Changes in legislation provided new authorities, including in 2001 ministerial authorizations for cyber defence activities that would risk intercepting private communications and in 2019 ministerial authorizations to protect non-federal electronic infrastructures, that drove the development of activities to strengthen the security of government systems

and eventually better defend them. At the same time, major cyber threat actors forced the government to adapt its defences, particularly following critical cyber incidents that caused significant loss of data and underlined the vulnerability of individual departments and the government more generally. The government responded by developing key strategies and policies, investing in the modernization of information technology and cyber defences, and creating organizations specifically tasked with addressing weaknesses in the system.

14. In the process, the government moved away from its siloed, department-by-department approach to cyber defence. It now treats the government as an 'enterprise,' where a few organizations are responsible for government-wide cyber defence. Central to this framework are three organizations: TBS, SSC and CSE. Nonetheless, this horizontal framework appears to be increasingly incompatible with the government's existing department-by-department 'vertical' authority structure outlined in the *Financial Administration Act.* This authority structure makes deputy heads ultimately responsible for ensuring the protection of their department's respective systems. It also gives them latitude to accept or reject TBS, CSE or SSC direction, putting at risk the overall efficacy of the cyber defence framework.

The Committee found that the strength of the government's cyber defence system is weakened by the inconsistent application of security–related responsibilities and the inconsistent use of cyber defence services.

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

16. Fourth, the Committee found that the strength of the government's cyber defence system is weakened by the inconsistent application of security-related responsibilities and the inconsistent use of cyber defence services. Put simply, not all federal organizations receive cyber defence protection. Most significantly, a number of federal organizations and interests are not subject to Treasury Board cyber-related directives or policies, and are therefore not obligated to obtain cyber defence services from government. Some of these organizations – including Crown corporations – have chosen not to receive government cyber defence services, leaving those organizations and the government as a whole at considerable risk from the most advanced cyber threats. Even among the federal organizations that do receive CSE cyber defence services, protection is inconsistent: organizations can select which services they would like to receive, while declining others. The Committee found that while SSC provides some cyber defence services to 160 of 169 federal organizations, only 43 of those organizations receive the full complement of SSC services.

17. The Committee made two recommendations to strengthen the government's cyber defence framework and extend that framework over federal government organizations as broadly as possible (see Annex B). First, the Committee recommended that the government continue to strengthen its framework for defending its networks from cyber attack by ensuring that its authorities and programs for cyber defence are modernized as technology and other relevant factors evolve. Second, the Committee recommended that the government apply relevant cyber defence policies, directives and services to all federal organizations to the greatest extent possible.

18. Together, the Committee's recommendations seek to ensure that government authorities are better aligned with the cyber defence 'enterprise' and that all federal organizations are brought within the government's secure perimeter and protected to the greatest extent possible.

19. The Committee was pleased to see that, for the first time, the government provided an official response to NSICOP recommendations. This is an important step in strengthening accountability and transparency.

Annex A: Cyber Defence Review Findings and Recommendations

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.

Findings

The Committee makes the following findings:

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

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

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

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

- Treasury Board policies relevant to cyber defence are not applied equally to departments and agencies. As a result, not all organizations must fulfill the same responsibilities, requirements and practices. This creates gaps in protecting government networks from cyber attack.
- Crown corporations and potentially some government Interests are known targets of state actors, but are not subject to Treasury Board cyber-related directives or policies and are not obligated to obtain cyber defence services from the government. This puts the integrity of their data and systems and potentially those of the government at significant risk.

- Cyber defence services are provided inconsistently. While Shared Services Canada provides some services to 160 out of 169 federal organizations, only 43 of those receive the full complement of its services. The Communications Security Establishment provides services in support of Shared Services Canada and through agreements with some individual organizations. This inconsistency introduces risks to those organizations and to the rest of government and limits the overall efficacy of CSE's cyber defence program.

Recommendations

The Committee makes the following recommendations:

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

R2. To the greatest extent possible, the government:

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

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 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 finds, 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

The Committee will seek a status update in 2022.

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

The Committee will seek a status update in 2022.

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

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

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.

The Committee recognizes that recommendation R2 was overtaken by events.

The Committee will seek a status update in 2022.

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

The Committee will seek a status update in 2022.

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

The Committee will seek a status update in 2022.

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

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.

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

The Committee makes the following 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

The Committee will seek a status update in 2022.

Annex C: The Review Process

Type of Review

Framework

A review of the legislative, regulatory, policy, administrative and financial framework for national security or intelligence.

Activity

A review of any activity carried out by a department that relates to national security or intelligence.

Review Criteria

For the Committee to consider a review, it must involve one core member of the security and intelligence community and:

- For national security issues, relate to threats to the security of Canada as defined in the CSIS Act or criminality of national scope and gravity,
- For intelligence issues, involve the use of clandestine, covert, or privileged sources or methods.

Review Considerations

Organization

- whether the organization was previously subject to review;
- the extent of its security or intelligence activities, and the degree to which they are known; and,
- whether the activities are governed by specific legislation or formal government direction.

General

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

Review Process

STAGE 1 – PROPOSALS FOR REVIEW

STEP 1 Consider range of topics for review

STEP 2 Select topics and identify implicated organizations

STEP 3 Notify Ministers and provide Terms of Reference

STAGE 2 – CONDUCT REVIEW

STEP 4 Receive and analyze information and follow-up with organizations

STEP 5 Consider interim report and determine direction

STEP 6 Conduct hearings with officials and subject matter experts

STEP 7 Develop draft report

STAGE 3 – FINAL REPORT

STEP 8 Provide report to implicated organizations for fact checking and comment

STEP 9 Consider organizational input and finalize report

STEP 10 Provide classified report to Prime Minister (PM) and implicated organizations

STAGE 4 – TABLING AND PUBLICATION

STEP 11 PM and Committee Chair discuss the report

STEP 12 On the advice of officials, the PM may direct the removal of injurious information

STEP 13 Committee revises the report

STEP 14 Report is tabled in Parliament, referred to House and Senate standing Committees

Abbreviations

Cabinet	Cabinet of Canada
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
GAC	Global Affairs Canada
GoC	Government of Canada
HoC	House of Commons
MND	Minister of National Defence
MPA	Minister of Public Safety
NSIA	National Security and Intelligence Advisor to the Prime Minister
NSIRA	National Security and Intelligence Review Agency
PCO	Privy Council Office
PMO	Office of the Prime Minister
PS	Public Safety Canada
RCMP	Royal Canadian Mounted Police
S&I community	Security and intelligence community
Sen	Senate
SSC	Shared Services Canada
TBS	Treasury Board of Canada Secretariat