The National Security and Intelligence Committee of Parliamentarians

2025 Annual Report

Canada

The National Security and Intelligence Committee of Parliamentarians

Annual Report 2025

CP100E (Print)
ISSN 2562-5101 (Print)

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

Cette publication est également disponible en français :
Rapport annuel 2025

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

Annual Report 2025

The National Security and Intelligence Committee of Parliamentarians

Message from the Committee

We are pleased to submit the eighth annual report of the National Security and Intelligence Committee of Parliamentarians to the Prime Minister. The past year brought notable changes for the Committee, beginning with the dissolution of the 44th Parliament in March 2025, which officially ended all Committee member appointments. Prime Minister Carney appointed a new Committee which includes four previous members and seven new members, the most since the very first Committee was named.

As a Committee, we recognize the important role we play in delivering independent, non-partisan review by legislators of national security and intelligence activities across the federal government. This mandate is especially vital in the face of evolving threats to Canada's security and sovereignty: the Committee's work is integral to providing a balance to the resulting increases in the resources and authorities of our national security and intelligence organizations. We look forward to building on the good work of previous Committees in fulfilling our mandate.

Since its appointment, the Committee has received comprehensive briefings and appearances from key organizations within the national security and intelligence community. Members remain actively engaged in resuming and concluding the review of the role of the National Security and Intelligence Advisor to the Prime Minister (NSIA), launched by the previous Committee in April 2024. The Committee also announced a new review focusing on Canada's counter terrorist financing framework in November, and looks forward to working with relevant Ministers, federal departments and organizations in the coming year.

Despite prorogation, the Committee presented both its 2024 Annual Report and the classified version of its *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations* to the Prime Minister in March 2025. Revised copies of both reports were tabled in Parliament in September 2025. The Committee is pleased to have received an official government response to its Special Report, included in Annex A of the Annual Report.

The Committee wishes to extend its thanks to the Secretariat staff for their dedicated service and vital assistance to the Committee in fulfilling its mandate. This Committee's review mandate improves the ability of the security and intelligence community to protect Canadians, upholds democratic principles and strengthens the accountability and effectiveness of Canada's national security and intelligence community. We look forward to continuing this invaluable work in service of Canadians.

The National Security and Intelligence Committee of Parliamentarians

(Membership from the 45th Parliament)

The Honourable Darren Fisher, P.C., M.P., Chair

The Honourable Claude Carignan, P.C., Senator

The Honourable Greg Fergus, P.C., M.P.

Rhéal Fortin, M.P.

Iqwinder Gaheer, M.P.

The Honourable Marty Klyne, Senator

Rob Morrison, M.P.

The Honourable Rebecca Patterson, OMM, MSM, CD, Senator

The Honourable Ginette Petitpas Taylor, P.C., M.P.

Alex Ruff, MSC, CD, M.P.

Abdelhaq Sari, M.P.

Table of Contents

Message from the Committee i

Introduction 1

The Committee's 2025 activities. 1

Reporting requirements for 2025 2

Other Reporting. 3

Special Report on the Lawful Access to Communications by Security and Intelligence Organizations 3

Annex A: Findings and recommendations of the Special Report on the Lawful Access to Communications by Security and Intelligence Organizations 5

Annex B: Outstanding recommendations of prior reviews 11

Annex C: Abbreviations. 13

Introduction

1. The National Security and Intelligence Committee of Parliamentarians (NSICOP or the Committee) is pleased to present the Prime Minister with its eighth annual report. The report provides an overview of the Committee's work over the past year. It also presents a summary of the Committee's *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations.*

The Committee's 2025 activities

2. The past year brought many changes for NSICOP, including dissolution of the Committee for the 2025 election and the subsequent appointment of a new Committee.
3. Parliament was prorogued from January 6, 2025 until March 24, 2025. Nevertheless, the previous Committee met several times during prorogation to finalize its special report on lawful access and the 2024 Annual Report.
4. The previous Committee submitted both the 2024 Annual Report and the classified version of its *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations* to the Prime Minister on March 4, 2025. Both reports were subsequently re-submitted to the new Prime Minister following the general election. Both the 2024 Annual Report and a revised version of the Committee's Special Report were tabled in Parliament on September 15, 2025. The Special Report is summarized below, and its findings, recommendations, and official government response are presented in Annex A.
5. The current Committee met ten times in 2025 and received comprehensive briefings and appearances from key organizations within the national security and intelligence community. The Committee decided to continue the review on the role of the National Security and Intelligence Advisor to the Prime Minister, recognizing and building upon work completed by the previous committee.
6. On November 24, 2025, NSICOP announced a review of Canada's framework for countering terrorist financing. A notification letter was sent to the Prime Minister and relevant Ministers. Initial requests for information have been sent to the appropriate federal departments and organizations.

Five-year review of NSICOP Act

7. The Committee wishes to highlight that the 5-year review of the *National Security and Intelligence Committee of Parliamentarians Act* (the NSICOP Act), adopted in 2017, remains overdue.
8. As outlined in Section 34 of the Act,

   > Five years after the day on which this Act comes into force, a comprehensive review of the provisions and operation of the Act is to be undertaken by the committee of the Senate, of the House of Commons or of both Houses of Parliament that is designated or established by the Senate or the House of Commons, or by both Houses of Parliament, as the case may be, for that purpose.

9. A comprehensive review would allow the Committee to make specific recommendations about reforming and updating the NSICOP Act. First, amendments to the NSICOP Act could improve the Committee's access to information and its ability to exchange information with other review bodies. Second, reforms could enhance the independence and efficiency of the Committee. It is important to the Committee that the Government refer the statutory review, now three years overdue, to the appropriate House of Commons or Senate committee.

Reporting requirements for 2025

Injury to national security and refusal to provide information

10. 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 prevented the Committee from conducting a review under paragraph 8(1)(b) of the Act because they determined that the review 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 its disclosure would be injurious to national security, consistent with subsection 16(1) of the Act.

11. In 2025, no reviews proposed by the Committee were deemed injurious to national security by a minister and no information requested by the Committee was refused to be disclosed by a minister on these grounds.

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

Avoiding Complicity in Mistreatment by Foreign Entities Act

12. 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.[1] The annual reports must contain information regarding:

- **a.** The disclosure of information to a 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.

[1] The federal organizations mandated to report are: 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; and Transport Canada

13. 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). The Committee received all twelve annual compliance reports.

Referrals

14. Pursuant to paragraph 8(1)(c) of the NSICOP Act, any minister of the Crown may refer a matter relating to national security or intelligence to the Committee for review. The Committee did not receive any referrals in 2025.

Other Reporting

15. The *Investment Canada Act* (ICA) enables the review of significant investments in Canada by non-Canadians that could be injurious to national security. The Minister of Industry may order further review of such an investment if, after consultation with the Minister of Public Safety and Emergency Preparedness, the Minister considers the investment may be potentially injurious. The Minister must disclose to NSICOP the outcome of a review that results in undertakings from investors accepted by the government or orders made by the Governor in Council under section 25.4 of the ICA.

16. The Minister may request any information deemed necessary for the review, and if the non-Canadian provides undertakings that nullify the injury to national security, the review concludes, and notice is given to the non-Canadian under s. 25.3(6)(c) of the ICA. The Minister must then notify NSICOP within 30 days of the identity of the non-Canadian and the business or entity that made the undertakings.

17. NSICOP received four s. 25.3(6)(c) notices in 2025. Copies of all notices are retained by the Secretariat of the NSICOP.

Special Report on the Lawful Access to Communications by Security and Intelligence Organizations

18. On September 15, 2025, the Prime Minister tabled a revised version of the Special Report on the *Lawful Access to Communications by Security and Intelligence Organizations* in both Houses of Parliament.

19. The Special Report examined the framework for lawful interception of communications by security and intelligence organizations. The report outlines the Committee's review of Canada's current legislative, regulatory, policy, and financial framework governing lawful access. It was published on the NSICOP website on the same day, containing eleven findings and seven recommendations.

20. Lawful access consists of the legally authorized interception of communications and collection of information and data by intelligence and law enforcement organizations

in their conduct of investigations. Law enforcement, security and intelligence bodies have argued that the demonstration of lawful access (i.e., a judicial warrant) cannot guarantee access to communications data, making access to vital information and evidence challenging. They have stated that this has significantly limited their ability to conclude investigations.

21. Challenges surrounding lawful access revolve around security and privacy considerations of individuals regarding their private communications, the role and power of the state to compel private corporations to provide unencrypted user communications data in response to lawful demands, and the need to protect both public and private communications and economic systems from digital threats. Civil liberty groups, privacy proponents, technologists and private corporations have argued that strong encryption is vital to the protection of personal and corporate information, and public data.

22. The review examined Canada's legal framework for lawful access, including relevant legislation such as the *Canadian Charter of Rights and Freedoms,* the *Criminal Code,* the *Canadian Security and Intelligence Service Act,* and the *Communications Security Establishment Act,* along with other relevant legislation such as the *Canada Evidence Act* and the *Privacy Act.*

23. The Committee explored the lawful access challenges security and intelligence agencies face in their investigations. It also examined the government's effectiveness in addressing or mitigating these challenges, and how it balances the need to support national security efforts while safeguarding Canadians' privacy rights. The Committee's assessment was based on its observations in these key areas.

24. The Committee heard from a wide range of witnesses, including ministers, government officials, civil society, privacy experts, and communications service providers (CSPs). The review examined information from January 1, 2012, to January 9, 2025 and included the following federal organizations: Canadian Security Intelligence Service (CSIS), Communications Security Establishment, Department of Justice, Department of Public Safety and Emergency Preparedness (Public Safety), and the Royal Canadian Mounted Police (RCMP).

25. The Committee found that CSIS and the RCMP face challenges in accessing digital communications content, attributed to rapid evolution and proliferation of communications technologies, the global nature of communications, and Canada's outdated legal framework. Canada does not have legislation to compel CSPs to ensure their systems are capable of intercepting communications and this gap causes investigative delays and financial inefficiencies for CSIS and the RCMP.

26. The Committee found that the RCMP faces additional challenges balancing the use of sensitive investigative techniques and the legal requirement to disclose them in court. As a result, they often avoid using these tools or risk losing the ability to use the resulting evidence in prosecutions. This is referred to as the intelligence to evidence dilemma.

27. The Committee concluded that lawful access challenges, if left unaddressed, would undermine Canada's national security in the long term by hampering the ability of CSIS and the RCMP to fulfil their respective mandates. Canada's inability to overcome these challenges may also hinder its capacity to contribute effectively to intelligence-sharing and joint threat responses within the Five Eyes alliance (Canada, U.S., U.K., Australia, and New Zealand).

Annex A: Findings and recommendations of the *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations*

Findings

F1. Canada's security and intelligence organizations do not systematically track how often they encounter technological challenges in their national security investigations and whether they are successful in mitigating these challenges.

F2. The RCMP and CSIS face significant challenges in accessing communications content, for which metadata is not necessarily a substitute.

F3. There was consensus across appearances that legislation to compel the creation of exceptional access or "backdoors" to encryption platforms was neither required nor desired.

F4. Canada's public position on lawful access to encrypted communication is unclear. National security practitioners, cybersecurity experts and privacy advocates do not have a common understanding of the problem.

F5. The government's failure to develop and implement a solution to the Supreme Court's decision in *Spencer* is impeding CSIS and the RCMP's ability to respond to national security threats.

F6. Without a general legal requirement on CSPs to retain metadata for a specified period of time, there is a risk that data sought pursuant to a warrant will be unavailable.

F7. The government's inability to make progress on the intelligence and evidence dilemma, particularly with respect to the protection of investigative techniques, has contributed to a situation in which the RCMP is forced to choose either to not use sensitive tools and techniques during an investigation because of the potential disclosure issues, or risk not being able to rely on evidence obtained through their use at trial or having a prosecution stayed because of a court order to disclose.

F8. The government lacks formal policies to address the procurement, regulation and use of commercial On-Device Investigative Tools, and ensure transparency in reporting with respect to their use by law enforcement and CSIS.

F9. The absence of legislation requiring communications service providers (CSPs) to maintain lawful intercept capability creates unnecessary risks for all stakeholders, including CSIS, federal, provincial, territorial and municipal law enforcement, CSPs and ultimately the Canadian public. It also impedes Canada's ability to work with international partners. The failure to address this issue at a strategic policy level

has resulted in operational agencies themselves developing foundational policies and procedures, notably compensation models, geared toward ensuring continued cooperation from CSPs, rather than a principled approach based on input from Ministers and Parliament.

F10. The risks associated with the absence of legislation requiring communications service providers to be intercept capable is compounded by the absence of a centralized national authority to coordinate, develop, and maintain lawful intercept capabilities in Canada.

F11. The Canada-U.S. Data Access Agreement would remove long-standing jurisdictional barriers to judicially-authorized access to U.S. communications service providers, including major social media platforms, without compromising privacy or encryption.

Recommendations

R1. Under the leadership of the Minister of Public Safety, the government develop and implement a comprehensive strategy to address Canada's lawful access challenges, drawing from the Committee's review and findings. Such a strategy should:

- Affirm key principles, such as legitimacy, necessity, and proportionality;
- Identify, track, and report on key lawful access challenges and associated risks;
- Include communications, stakeholder engagement and transparency commitments; and
- Consider challenges that may arise due to emerging technology, e.g., artificial intelligence.

R2. The government publicly clarify its position on exceptional access to communications information protected by encryption.

R3. The government table legislation creating new authorities in the *Canadian Security Intelligence Service Act* and the *Criminal Code* to enable the production of basic subscriber information, and the government consider legislation with respect to data retention.

R4. Further to the Committee's 2024 recommendation in its *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* that the government address intelligence and evidence challenges, the government develop and implement a solution to address concerns about the protection of investigative tools, which may include revisions to the relevant provisions of the *Canada Evidence Act.*

R5. The government develop policies and guidelines on the procurement, use and reporting requirements for commercial On-Device Investigative Tools.

R6. The government table legislation to compel intercept capability for communications service providers (CSPs). The legislation should be encryption neutral and not include a decryption requirement. The government must also decide on a compensation model for compliance costs, i.e., whether CSPs should be compensated for the development, maintenance, and operating costs associated with lawful access. The legislation should:

- establish and identify the national authority (i.e., the National Lawful Access Centre) for the coordination of lawful interception initiatives;

- define communications service provider so as to include any service provider operating in Canada offering electronic communications services or capabilities;
- define intercept capability to include support for computer network exploitation; and
- set mandatory technical standards, including those related to cybersecurity.

R7. The government prioritize the signing and implementation of the Canada-U.S. Data Access Agreement.

Status

28. The government provided an official response to all recommendations for the 2025 Annual Report. The government agreed to 5 of the recommendations and partially agreed with R5 and R6.

Response to R1

The Government recognizes the growing complexity of criminal and national security threats and agrees with the recommendation. A comprehensive strategy to address lawful access challenges would ensure that law enforcement and the Canadian Security Intelligence Service (CSIS) have the tools they need to lawfully access electronic information in support of their investigations into these threats while upholding Canadians' privacy rights and freedoms.

As a first step, the Government introduced the *Strong Borders Act* (the Bill) on June 3, 2025.

Part 14 of the Bill, *Timely Access to Data and Information,* proposes to amend the *Criminal Code* to address domestic issues such as timely responses to legally authorized requests for subscriber information by law enforcement. Parallel changes in the *CSIS Act* will permit parallel powers for national security. Part 14 would update existing tools to facilitate access to data and information that is especially important in the early stages of criminal and national security investigations. Part 14 would also amend the *Mutual Legal Assistance in Criminal Matters Act* to provide a further tool of international cooperation for Canadian and foreign partners to obtain the production of subscriber information or transmission data.

Part 15 of the Bill, the *Supporting Authorized Access to Information Act* (SAAIA), would compel select electronic service providers (ESPs) to develop and maintain capabilities to support law enforcement agencies and CSIS by having systems that give effect to legal authorizations for access to information.

The Minister of Public Safety, in collaboration with partners and stakeholders, will explore how best to address other components of the recommendation not covered by Parts 14 and 15 of the Bill, including tracking, reporting transparency and emerging technology.

Response to R2

The Government agrees with the recommendation to clarify its position on exceptional access to communications information protected by encryption. The Government recognizes that encryption is important to safeguard cybersecurity, privacy, and economic security, but also poses significant challenges in the course of criminal and intelligence investigations.

Cyber security and privacy concerns are at the forefront of lawful access and the Government recognizes that the creation of "backdoors" could weaken cybersecurity, increasing the risk that threat actors could also leverage these "backdoors" to access data and compromise the privacy of Canadians. As such, the Government does not support the implementation of measures that could create vulnerabilities in electronic protections (e.g., encryption and authentication).

The *Supporting Access to Authorised Information Act* (Part 15 of the *Strong Borders Act*) includes explicit provisions to ensure that ESPs would not be obliged to implement regulatory requirements or Ministerial Orders that would introduce systemic vulnerabilities (e.g., "backdoors") in electronic protections or to prevent a provider from rectifying such a vulnerability.

Response to R3

The Government agrees with the recommendation to table legislation creating new provisions in the *CSIS Act* and the *Criminal Code* to enable the production of subscriber information.

To address this gap, Part 14 of the *Strong Borders Act* proposes amendments to the *CSIS Act* and the *Criminal Code* to ensure that CSIS and law enforcement have the necessary and appropriate authorities to obtain subscriber information and data in a timely manner.

The Government also agrees with the recommendation to consider legislation for data retention. In consultations with partners and stakeholders, the government will explore the issue, taking into account various factors such as privacy and cybersecurity implications, to determine the best approach.

Response to R4

Canadians expect their government to ensure public security, effectively enforce laws and afford fair trials to those accused. The Government recognizes that the disclosure of sensitive details about investigative tools and techniques impacts law enforcement and national security agencies' ability to use them in other investigations. The Government also recognizes the importance of balancing the right to a fair trial with the need to protect classified investigative techniques. The Government will aim to update the approach to the current legislative framework in order to have the ability to adapt to the fast-evolving digital landscape.

It should also be noted that the *Canada Evidence Act,* recently amended as part of Bill C-70, provides for Secure Administrative Review Proceedings (SARP) in Federal Court. SARP improves and standardizes legal procedures and protections for sensitive information when used in administrative decisions that are subject to judicial review. This is a preliminary step towards a justice system that is better equipped to consider classified evidence.

Response to R5

The Government recognizes the importance of On-Device Investigative Tools (ODITs) used by law enforcement and CSIS in support of investigations.

The Government partially disagrees with this recommendation as both CSIS and the RCMP already have safeguards in place to regulate the use, procurement, and reporting on these types of tools; including judicial authorization and clear internal governance structures.

For example, CSIS obtains warrants from the Federal Court authorizing the deployment of ODITs, which ensures judicial control over their permitted use. CSIS also established the Operational Technology Review Committee (OTRC) in 2020. The OTRC's mandate is to review new technologies and the novel uses of existing ones that are proposed to be deployed as part of CSIS's collection mandate. Any proposals to procure or use new technologies in relation to ODITs fall within scope of OTRC's mandate. The OTRC includes representation from relevant stakeholders, to ensure that risks are thoroughly considered assessed when considering these technologies.

In the case of the RCMP, a Superior Court judge must approve and issue an authorization, informed by a technical brief describing the proposed techniques. Conditions restricting the collection of communications are often imposed as part of the authorization. The RCMP created the National Technology Onboarding Program (NTOP) in 2021 to create a centralized system to identify, assess, and track new and emerging investigative tools and technologies used by the RCMP, providing greater transparency.

Furthermore, in partnership with Global Affairs Canada, the RCMP is exploring Canada's involvement in the Pall Mall process, an international initiative led by the United Kingdom and France, which enlists governments, private sector, and civil society to establish guidelines and principles to address challenges posed by the potential proliferation and irresponsible use of commercial cyber intrusion capabilities. Since 2020, the RCMP has provided an annual report to the Minister of Public Safety on its use of electronic surveillance which includes statistics. Additionally, the RCMP has provided the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI) statistics on its use of ODITs, which can be found at:

https://www.ourcommons.ca/content/Committee/441/ETHI/WebDoc/WD11922842/11922842/RoyalCanadianMountedPolice-DeploymentStats-e.pdf.

In November 2022, ETHI published the, "Device Investigative Tools Used By The Royal Canadian Mounted Police And Related Issues" report, which is available at:

https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf.

While mitigation strategies and measures have been put in place at both CSIS and the RCMP, the government recognizes the need for consistency across departments. Public Safety, in collaboration with CSIS, CSE, Justice and the RCMP will conduct an assessment of existing organizational policies and guidelines to identify gaps and determine how best to operationalize the recommendation.

Response to R6

The Government recognizes that the current framework has not kept pace with advancements in digital communication and technology. Communication networks have become more complex due to the rise of mobile and Internet communications, messaging platform, service resellers, Cloud hosting services, and emerging network technologies. Consequently, service providers are not always able to give effect to legally authorized information and intercept requests.

The Government agrees with the recommendation and has introduced the *Supporting Authorized Access to Information Act* (SAAIA), Part 15 of the *Strong Borders Act,* to compel select electronic service providers to develop and maintain capabilities to support law enforcement agencies and CSIS by having systems that give effect to legal authorizations for access to information. The SAAIA includes explicit provisions to ensure that ESPs would not be obliged to implement regulatory requirements or Ministerial Orders that would introduce systemic vulnerabilities in electronic protections, (e.g., encryption and authentication), or to prevent a provider from rectifying such a vulnerability. Specific obligations for select ESPs will be defined in regulation.

While the government recognizes the value of a centralized national authority for the coordination of lawful access, it disagrees with the need to establish it in legislation. A National Lawful Access Centre can be stood-up without enshrining the organization in law.

Response to R7

The Government of Canada will continue discussions with the United States on the Canada-US Data Access Agreement. As well, Part 14 of the *Strong Borders Act* introduces amendments to the *Criminal Code* and the *Mutual Legal Assistance in Criminal Matters Act* that add investigative tools for Canadian and foreign law enforcement authorities to obtain transborder subscriber information and transmission data through more efficient means.

Annex B: Outstanding recommendations of prior reviews

Special Report on the National Security and Intelligence Activities of Global Affairs Canada

Description

The report provides an overview of the nature and scope of the national security and intelligence activities at Global Affairs Canada. It examines the authorities under which the Department conducts those activities and how it governs them to support the accountability of the Minister of Foreign Affairs. It describes the structures the Department has in place to try to ensure that the activities and policies of other organizations with security and intelligence responsibilities align with Canada's foreign policy objectives. Finally, the report highlights areas where the Department plays a leadership role in the government, including two recent case studies of terrorist hostage takings abroad.

Recommendations

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

For the 2024 Annual Report, the government provided a response and status update on the implementation of some recommendations, but did not provide an official response for R4 regarding a framework on terrorist hostage takings. The government then provided an official response to R4 for the 2025 Annual Report.

Response to R4

A framework for the Government of Canada's response to terrorist hostage-taking has been developed in consultation with the eight departments and agencies which form the Interdepartmental Task Force (IDTF) on International Critical Incidents. GAC aims to institutionalize the framework through cooperation agreements and MOUs amongst IDTF member departments. GAC has also advanced professionalization in the provision of these specialized services, providing training to over 160 GoC officials since NSICOP's review of this activity.

Diversity and Inclusion in the Security and Intelligence Community

Description

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

Recommendations

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

For the 2025 Annual Report, the government provided a response and status update regarding the Committee's recommendation to develop a common performance measurement framework to strengthen accountability for diversity and inclusion.

Response to R4

A common performance measurement framework was considered. However, departments and agencies have individual Employment Equity Plans, which include goals and indicators. Departments and agencies continue to enhance and update their Plans, including developing performance measurement frameworks and measuring performance in addressing areas of under-representation. The Office of the Chief Human Resources Officer has recently issued guidance on how to develop performance indicators; departments and agencies will update their indicators as required.

Every department and agency within the security and intelligence community is operating within a particular set of circumstances, and has a unique role that requires different skillsets and experiences. Departments and agencies' individual performance measurement frameworks take into consideration the diversity between them in terms of labour needs, recruitment strategies, and specific gaps that they may need to address individually. A common community framework is unlikely to capture these differences effectively, and thus may not be able to address diversity and inclusion issues as well as individual departmental frameworks.

Annex C: Abbreviations

CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSP	Communications service provider
DOJ	Department of Justice
ESP	Electronic Service Provider
ETHI	House of Commons Standing Committee on Access to Information, Privacy and Ethics
GBA+	Gender-based Analysis Plus
ICA	Investment Canada Act
IDTF	Interdepartmental Task Force
NSIA	National Security and Intelligence Advisor to the Prime Minister
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
NTOP	National Technology Onboarding Program
ODITS	On-Device Investigative Tools
OTRC	Operational Technology Review Committee
RCMP	Royal Canadian Mounted Police
SAAIA	Supporting Authorized Access to Information Act
SARP	Secure Administrative Review Proceedings
UK	United Kingdom
US	United States of America