National Security and Intelligence Review Agency | Office de surveillance des activités en matière de sécurité nationale et de renseignement

Canada

NSIRA

2023 // Annual Report



© His Majesty the King in Right of Canada, as represented
by the National Security and Intelligence Review Agency, 2024.
ISSN 2563-5778
Catalogue No. PS106-9E-PDF

September 26, 2024

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister and Privy Council
Ottawa, ON
K1A 0A2

Dear Prime Minister,

On behalf of the National Security and Intelligence Review Agency, it is my pleasure to present you with our fifth annual report. Consistent with subsection 38(1) of *the National Security and Intelligence Review Agency Act*, the report includes information about our activities in 2023, as well as our findings and recommendations.

In accordance with paragraph 52(1)(b) of the *National Security and Intelligence Review Agency Act*, our report was prepared after consultation with the deputy heads concerned in an effort to ensure that it does not contain information whose disclosure would be injurious to national security, national defence, or international relations, or information that is subject to solicitor-client privilege, the professional secrecy of advocates and notaries, or to litigation privilege.

Yours sincerely,



The Honourable Marie Deschamps, C.C.

Chair // National Security and Intelligence Review Agency

Table of contents

Message from the members iii

Executive summary v

01 // Introduction 1

1.1 Mandate 1

02 // NSIRA's first five years 3

03 // Value of expanded partnerships 8

04 // Reviews 12

4.1 Overview 12

4.2 Canadian Security Intelligence Service reviews 14

4.3 Communications Security Establishment reviews 21

4.4 Other department reviews 30

4.5 Multi-departmental reviews 33

05 // Complaint investigations 36

5.1 Overview 36

5.2 Ongoing initiatives 37

5.3 Investigation summaries 38

5.4 Statistics on complaints investigations 44

06 // Conclusion 46

07 // Annexes 47

Annex A: Abbreviations 47

Annex B: Review findings and recommendations 50

Annex C: Statistics on complaints investigations 69

Message from the members

As members of the National Security and Intelligence Review Agency (NSIRA), we are pleased to present our 2023 Annual Report, marking the five-year milestone of our agency's journey. This report encapsulates our activities of the past year and provides an opportunity for reflection on the progress and evolution of our agency since 2019.

As world events have unfolded, and the pace of security and intelligence activities has advanced, the presence of our agency has never been more important. Since NSIRA's inception, our mandate has been to provide independent oversight and accountability of Canada's national security and intelligence activities. Over the last five years, we have brought greater transparency on such activities to the Canadian public, and we are proud of the strides we have made in fulfilling this crucial role.

Our agency has matured and strengthened in many ways. We have built enhanced capacity to conduct thorough and effective reviews and investigations of our country's diverse range of national security and intelligence activities. We have assembled a team of dedicated professionals with a wealth of expertise in numerous fields, enabling us to address complex issues and provide informed assessments and recommendations.

We have also fostered constructive relationships with our reviewees, partner agencies, parliamentary committees, and civil society organizations. These partnerships have been instrumental in facilitating our access to information, engagement in meaningful dialogue, and our ability to promote transparency and accountability.

Over the last five years, we have enhanced public awareness and understanding of the critical issues at stake in the realm of national security and intelligence. Through the publication of our reports, we have sought to demystify this often-opaque domain and empower Canadians to participate in informed discussions about their security and rights.

As we reflect on our achievements to date, we are mindful of the challenges that lie ahead. The landscape of national security and intelligence is constantly evolving as emerging threats and technological advancements present new challenges. As adaptive and agile responses are required by Canada's security and intelligence agencies, NSIRA will continue to assess whether such responses are lawful, reasonable, and necessary.

Looking ahead, we are committed to continuing our vital work. We remain dedicated and vigilant in our role of ensuring that Canada's national security and intelligence framework remains

accountable, and reporting on whether national security or intelligence activities are respectful of the rights and freedoms of all Canadians.

We extend our gratitude to all Secretariat staff, past and present, whose dedication and support has contributed to NSIRA's evolution over the past five years. Their efforts have been invaluable in shaping our agency and our work serving the Canadian public.

Marie Deschamps	Marie-Lucie Morin	Foluke Laosebikan	Jim Chu
Craig Forcese	Matthew Cassar	Colleen Swords	

Executive summary

1. 2023 marked a momentous year for the National Security and Intelligence Review Agency (NSIRA). Relentless efforts to mature the agency's processes and professionalize its approaches allowed NSIRA to conduct its reviews and investigations to the highest standards. This report highlights the significant outcomes achieved through refined methodologies, strengthened partnerships, and an unwavering commitment to all Canadians to provide accountability and transparency of the national security and intelligence activities of the Government of Canada.

NSIRA's first five years

2. NSIRA celebrated its fifth anniversary in July 2024 and has used this as an opportunity to reflect on its growth and development, as well as lessons learned. The agency has embraced its broad and unique mandate, completing reviews that span organizations and increasing its transparency in implementing its investigations mandate. NSIRA has prioritized the growth and development of its staff, enhanced review literacy across reviewed entities, and continued to maintain best practices and the highest standards in implementing its mandate.

Value of expanded partnerships

3. NSIRA has expanded and leveraged its network of oversight partners through its numerous engagements with international counterparts and participation in international forums in 2023. This has benefitted all parties through sharing best practices, lessons learned, expertise, and research. NSIRA's integration into the international community of national security and intelligence oversight has advanced the agency's development and enhanced its capacity to carry out its mandate.

Reviews

4. The following are highlights and key outcomes of the reviews NSIRA completed in 2023. (Ongoing reviews are not included.) Annex B lists all the findings and recommendations associated with reviews completed in 2023.

Canadian Security Intelligence Service

5. NSIRA completed the following reviews where Canadian Security Intelligence Service (CSIS) activities were solely at issue:

    - a review of CSIS' Dataset Regime, which examined its implementation, including aspects of governance, information management, retention practices, and training; and
    - an annual review of CSIS' activities, which informed, in part, NSIRA's 2023 classified annual report to the Minister of Public Safety.

Communications Security Establishment

6. NSIRA completed the following reviews where Communications Security Establishment (CSE) activities were mostly at issue:

    - a review on CSE's use of the polygraph for security screening, which examined the way CSE operated its polygraph program and the role of the Treasury Board of Canada Secretariat (TBS) in establishing the Standard on Security Screening that governs the use of the polygraph for security screening by the Government of Canada;
    - a review of CSE's network-based solutions and related cybersecurity and information assurance activities, which was NSIRA's first review of these activities, as well as its first review of Shared Services Canada (SSC); and
    - an annual review of CSE's activities, which informed, in part, NSIRA's 2023 classified annual report to the Minister of National Defence.

Canada Border Services Agency

7. NSIRA completed a review of the Canada Border Services Agency's (CBSA's) Confidential Human Source (CHS) program, which examined the legal and policy frameworks governing the program, with particular attention to the management and assessment of risk; the agency's discharge of its duty of care to its sources; and the sufficiency of ministerial direction and accountability in relation to the program.

Department of National Defence and the Canadian Armed Forces

8. NSIRA completed a review of the Department of National Defence (DND) and Canadian Armed Forces' (CAFs) Human Source Handling program, which examined whether DND/CAF conducts its human source-handling activities lawfully, ethically, and with appropriate accountability.

Multi-departmental reviews

9. NSIRA completed a review of the operational collaboration between CSE and CSIS, which was NSIRA's first review to examine the effectiveness of the collaboration by assessing their respective mandates and associated prohibitions. This review also satisfied NSIRA's annual requirement under section 8(2) of the *National Security and Intelligence Review Agency Act* (NSIRA Act) to review an aspect of CSIS' threat reduction measures (TRMs).

10. NSIRA completed two mandated multi-departmental reviews in 2023:

    - a review of directions issued with respect to the *Avoiding Complicity in Mistreatment by Foreign Entities Act*; and
    - a review of disclosures of information under the *Security of Canada Information Disclosure Act* (SCIDA).

Complaint investigations

11. The NSIRA Secretariat – in consultation with NSIRA members – established service standards for complaint investigations and set the goal of completing 90 percent of cases within the service standards. This commitment supports NSIRA's complaint investigations by ensuring timeliness. NSIRA also implemented an independent verification process for complaints against CSE. Additionally, the agency completed a study on the collection of race-based data and other demographic information.

12. NSIRA observed an increase of complaints against CSIS, pursuant to section 16 of the NSIRA Act, alleging process delays in immigration or citizenship security screening.

01 //

Introduction

1.1 Mandate

13. The National Security and Intelligence Review Agency (NSIRA) is an independent agency that reports to Parliament and has the authority to conduct an integrated review of Government of Canada national security and intelligence activities. This provides Canada with one of the most extensive systems for independent review of national security in the world. NSIRA has a dual mandate: to conduct reviews, and to carry out investigations, of complaints related to Canada's national security or intelligence activities. In fulfilling its mandate, the agency is assisted by a Secretariat headed by an Executive Director.

Reviews

14. NSIRA's review mandate is broad, as outlined in subsection 8(1) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).[1] This mandate includes reviewing the activities of the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), as well as those of any other federal department or agency that are related to national security or intelligence.[2] The agency may also review any national security or intelligence matter that a Minister of the Crown refers to NSIRA.[3]

Investigations

15. NSIRA is responsible for investigating complaints related to national security or intelligence. This is outlined in paragraph 8(1)(d) of the NSIRA Act, and involves investigating the following:

    - complaints about the activities of CSIS or CSE;

[1] The *National Security and Intelligence Review Agency Act* (S.C. 2019, c. 13, s. 2) is available at https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html.
[2] See Annex A for a complete list of abbreviations used in this report.
[3] Further information on NSIRA's mandate, including previous annual reports, is available at https://nsira-ossnr.gc.ca.

- complaints referred to it by the Civilian Review and Complaints Commission (CRCC)[4] about the conduct of the Royal Canadian Mounted Police (RCMP) insofar as they relate to national security;
- complaints related to decisions to deny or revoke federal government security clearances;
- matters referred to it under the *Canadian Human Rights Act*; and
- ministerial reports under the *Citizenship Act* that recommend denying certain citizenship applications.

[4] The RCMP's own complaints mechanism is available at https://www.crcc-ccetp.gc.ca.

02 //

NSIRA's first five years

A new era of security and intelligence accountability in Canada

16. The conversation on national security and intelligence issues is evolving in Canada. In recent years, armed conflicts, the COVID-19 pandemic, and activities of foreign and domestic security and intelligence agencies have all been featured in news headlines. Most recently, Parliament debated the role of Canada's security and intelligence agencies in responding to the threat of foreign political interference. The importance of robust review and oversight has never been more clear or timely. As the conversation grows, Canadians will want more information about the functioning of their security and intelligence systems. NSIRA is the trusted eyes and ears of Canadians, providing transparency that did not previously exist.

17. NSIRA's mandate is to review issues and conduct investigations of complaints related to Canada's national security or intelligence activities. Prior to NSIRA, although some activities were subject to review, no single agency had the mandate and authority to review activities across the national security and intelligence landscape, and some departments lacked an independent review body.

18. The siloed framework limited NSIRA's predecessor agencies, the Security and Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner to reviews and investigations of complaints within their narrow mandates. For example, reviews did not trace the progression of an issue as it traversed government departments.

A unique mandate

19. NSIRA's broad mandate is unique within the international community, providing a much greater understanding of how departments and agencies work and interact in the national security and intelligence space. For example, in 2023, NSIRA launched a review of the dissemination of intelligence on foreign interference, focusing on how intelligence progressed from departments charged with collecting intelligence through to its ultimate consumers. Such a review was not possible for NSIRA's siloed predecessors.

20. NSIRA's reviews have involved 19 departments and agencies to date. Its expanded mandate for investigating complaints encompasses those against CSIS, CSE and, upon referral, those from the CRCC concerning the RCMP and the Canadian Human Rights Commission (CHRC). NSIRA's work gets to the heart of how national security and intelligence activities are conducted, allowing for precise and effective recommendations.

Building processes and excellence from the ground up

21. NSIRA has prioritized professionalizing how it conducts reviews by developing policies and processes to support the review process. These were created even as the agency was growing and delivering on its complex mandate, and through the COVID-19 pandemic.

22. NSIRA has also modernized its policies and processes for its investigations of complaints. The agency undertook significant reform of its investigative process and published new *Rules of Procedure* to replace the previous model, increasing procedural transparency for those involved in the complaints process. When the COVID-19 pandemic made in-person hearings impossible, NSIRA pivoted and introduced alternate solutions, such as conducting its investigative interviews over video conference, thereby retaining access for participants.

23. NSIRA has built a proactive disclosure practice to publish its reports on its website. It has also undertaken an effort to publish those prepared by SIRC, to the greatest extent possible. The goal is to make NSIRA's reviews and its findings and recommendations available to the public as soon as possible. Proactive disclosure increases transparency and contributes to the dialogue on national security and intelligence in Canada.

Empowering professionals

24. The Secretariat is now staffed by almost 100 full-time employees. NSIRA's greatest asset is its people, and the Secretariat continues to attract staff with a range of expertise in research, review, technology, and law. This breadth has resulted in a diversity of reviews and a professionalized investigative model for addressing complaints.

25. NSIRA has actively developed a unique culture and is innovative in how it manages its review process. Review teams are comprised of individuals with diverse skill sets that reflect the need for legal and technical expertise. Teams are responsible for executing reviews under the direction of NSIRA members, with the guidance and support of Secretariat management. The result is detailed, fearless reviews.

26. Similarly, NSIRA's model for investigations of complaints is now designed for NSIRA members to be expertly supported by legal, registry, and research staff. This enhances members' effectiveness in their adjudicative role conducting investigations.

The challenge of more effective review

27. NSIRA's mission is to serve as the trusted eyes and ears of Canadians through independent, expert review and investigation of the Government of Canada's national security and intelligence activities. To successfully implement its mission, NSIRA must select the right reviews and have access to the required information.

28. The NSIRA Act requires NSIRA to conduct certain annual reviews; it also gives the agency discretion to choose topics to review. This discretion is fundamental as NSIRA must be able to "follow the thread" to ensure that activities deserving scrutiny are independently reviewed. Specifically, NSIRA has developed a review planning and consideration matrix, consisting of formal criteria that help identify review topics in accordance with NSIRA's core mandate and mission. The prioritization of reviews is informed by additional strategic factors, including assessments of the nature of the activity and the compliance risk its poses, the novelty of the activity and any technology it employs, as well as resourcing, ongoing reviews, and public interest.

29. Access to information is the lifeblood of review, and NSIRA continues to insist upon its access rights. Effective review requires timely and complete responses to NSIRA's requests for information, open and candid briefings, and mutual respect. Despite the agency's unfettered access under the NSIRA Act, navigating access issues has not been without its struggles. There has been a learning curve, for both reviewed entities and NSIRA, and increasing review literacy in the departments and agencies under NSIRA's review mandate is an ongoing priority.

Successes of NSIRA's mandate

30. NSIRA's impact on the national security and intelligence community extends beyond that of the reviewed departments. Recently, the Federal Court released a decision on a CSIS warrant matter that used an NSIRA report to inform its background and analysis. The Court considered the issues identified by NSIRA to be important in relation to the sharing of information collected under certain warrants.

31. Additionally, Ministers accountable for the security and intelligence community's activities have recognized the value of independent review and have referred matters to NSIRA. The first of

such reviews stemmed from a Federal Court judgment.[5] As a result, the Ministers of Public Safety and Justice referred the matter to NSIRA. NSIRA's report made findings and recommendations on Justice's provision of legal advice, CSIS and Justice's management of the warrant acquisition process, and broader cultural and governance issues.

32. Since 2019, NSIRA has completed 39 reviews (13 statutory and 26 discretionary)[6]. Of these reviews, 21 involved more than one department. NSIRA has also issued 17 different compliance reports to responsible Ministers, as required under section 35 of the NSIRA Act, whenever the agency finds that an activity may not be in compliance with the law.[7] Compliance issues range from a department missing a deadline prescribed in legislation to a potential Charter violation. NSIRA's reports have included more than 200 recommendations, ranging from specific process changes to wide-ranging structural reform. NSIRA has also received more than 200 complaints, highlighting the importance of accessibility to an independent investigation process to address complaints concerning the activities of CSIS, CSE, and the RCMP.

Looking ahead

33. As NSIRA looks to its future, it will also turn attention inward to ensure NSIRA's structure and governance is fit for purpose. The upcoming legislative review of the NSIRA Act provides the opportunity to make any required improvements.

34. NSIRA is immensely proud of its contributions to the scrutiny and transparency of Canada's security and intelligence activities during its first five years. It has played a pivotal role in ensuring there is independent accountability for the organizations involved in Canada's security and intelligence activities. As NSIRA looks ahead, it does so with enthusiasm and a renewed mission. NSIRA has recently codified its approach by formalizing its vision, mission, and values statements, and while the formal statements may be new, the underlying elements have provided the agency's foundation from its beginning.

---

[5] This was a judgement calling for a comprehensive external review be initiated to fully identify systemic, governance, and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it has conceded was illegal and the resultant breach of candor.

[6] Includes reviews with final reports approved by NSIRA members and sent to applicable ministers. Does not include classified annual reports sent the Minister of National Defence, and the Minister of Public Safety, or other review activities.

[7] More information on NSIRA's section 35 reporting is available at https://nsira-ossnr.gc.ca/en/reviews/policies-and-procedures/agency-application-of-sections-35-and-40-of-the-nsira-act.

NSIRA's Mission, Vision, and Values



03 //

Value of expanded partnerships

Expanded international partnerships and cooperation

35. Under NSIRA's predecessors, international partnerships were primarily established through the Five Eyes Intelligence Oversight and Review Council (FIORC),[8] which continues to be a foundational alliance for NSIRA. In addition to reinforcing and building upon the relationships it inherited, NSIRA has cultivated new partnerships with foreign counterparts and actively participated in international forums. In 2023 alone, NSIRA engaged with the following organizations and attended the following events:

    Organizations:

    Australia's Inspector-General of Intelligence and Security (IGIS Australia)
    New Zealand's Inspector-General of Intelligence and Security (IGIS New Zealand)
    The United States of America's Inspector General of the Intelligence Community (IC IG US)
    The United Kingdom's Investigatory Powers Commissioner's Office (IPCO UK)
    The United Nations' Counter-Terrorism Executive Directorate (UNCTED)
    The United States Privacy and Civil Liberties Oversight Board (PCLOB US)
    The Norwegian Parliamentary Oversight Committee on Intelligence and Security Services (EOS Norway)
    The Danish Intelligence Oversight Board (TET Denmark)
    The Independent Oversight Authority for Intelligence Activities of Switzerland (OA-IA)
    The German Parliamentary Oversight Panel (PKGr)
    The Dutch Review Committee on the Intelligence and Security Services (CTIVD Netherlands)

    Events and forums:

    Five Eyes Intelligence Oversight and Review Council Conference
    International Intelligence Oversight Forum
    European Intelligence Oversight Conference

Lessons learned and lessons shared with international partners

36. Connecting with international counterparts and participating in multilateral discussions has enabled NSIRA to tap into a network of partners. Relevant information is shared regarding best

[8] FIORC comprises agencies with an oversight and review mandate concerning national security activities in their respective countries (Canada, Australia, New Zealand, the United Kingdom, and the United States).

practices, methodologies, recent developments, and common issues. Information sharing and cooperation in the traditionally esoteric and insulated field of national security oversight has broadened NSIRA's outlook and informed its expectations with respect to the departments and agencies that it oversees.

37. NSIRA has found that many of the challenges it faces have been experienced, and in some cases overcome, by international partners. These include challenges that are operational in nature, such as tactics for acquiring and verifying information, and those that relate to NSIRA's Secretariat, such as the recruitment, training, and retention of staff. Leveraging the lessons learned by our international counterparts has accelerated NSIRA's own development and contributed to the agency's growing reputation as an exemplar in the realm of national security and intelligence oversight.

38. While certainly a voracious consumer of best practices, NSIRA is an equally active contributor. The agency has reciprocally shared its own unique approaches, processes, and methods with the broader oversight community, which in some instances has led partner organizations to follow NSIRA's lead and adopt its practices. Even where NSIRA has not been confronted with a specific issue firsthand, its perspective has been sought and acted upon by partners that recognize NSIRA's wealth of experience and renown for innovation.

39. Continuous and repeated engagements with international partners have allowed for working-level relationships to take root, flourish, and bear fruit in the form of both regularly scheduled touch points and casual, ad hoc, file-specific exchanges. Lowering the institutional barriers has promoted the exchange of expertise, had a more direct impact on the substantive work of each institution, and produced more tangible outcomes, as described in the examples below.

Examples of value gained from engagements

Benefits to NSIRA

- Through an extended assignment to NSIRA, a communications expert from IPCO UK conducted a wholistic assessment of the agency's current communications posture and played a critical role in crafting an inaugural communications strategy. The implementation of this strategy has helped NSIRA reach and build connections with domestic stakeholders. NSIRA's members and Secretariat staff are deeply grateful for the expert's contributions during their time with the agency.
- TET Denmark and EOS Norway were influential in the development and use of a new IT system review inspection, first used as part of NSIRA's Review of the Lifecycle of CSIS'

Warranted Information. They also contributed to functional and performance benchmarking used by NSIRA in its methodologies, common practices, and assessment criteria.

- NSIRA has consulted the American Inspector General to improve the responsiveness of reviewed departments and agencies to NSIRA's recommendations. NSIRA has begun adopting best practices for ensuring there is follow-up on recommendations it has provided.

NSIRA's contributions

- At an event hosted by Global Affairs Canada (GAC) as part of Canada's work in cooperation with the UNCTED, NSIRA gave a presentation to the UNCTED delegation to explain the role that independent review plays in assessing the legality of Canadian activities in the counter-terrorism realm. This showcased to international assessors how the Canadian model has built robust independent mechanisms for review of counter-terrorism operations that reaches both law enforcement and the intelligence service.
- NSIRA's review planning and consideration matrix was shared with New Zealand's IGIS, TET Denmark, and several other international partners. Following their visit to NSIRA, TET Denmark has updated its IT standards to include quality assurance steps and added additional factors to its risk assessment framework.

Greater collaboration leads to greater accountability

40. Just as security and intelligence agencies regularly cooperate and share information with international partners, so too must the bodies that oversee them. Collaboration among NSIRA and its foreign counterparts has produced, and continues to yield, mutual benefits for all parties involved. As a result, NSIRA has become a more capable organization with greater visibility in the transnational security and intelligence community, ensuring effective and exhaustive accountability of Canada's national security apparatus.

41. Domestically, within Canada's review and oversight community, NSIRA brings a distinct and valued perspective, filling a previously unoccupied space in this important network. As such, the agency complements the activities of its peers. In 2023, NSIRA met with numerous Agents of Parliament, including the Auditor General of Canada, the Public Sector Integrity Commissioner, and the Privacy Commissioner. The multi-decade institutional experience and maturity of these agents and their respective offices has proven to be invaluably instructive for NSIRA, and the exchange of best practices has been extremely helpful, particularly in the development of the Secretariat's communications capacity.

42. As provided for in the NSIRA Act, NSIRA engages with other oversight bodies to deconflict on issues of mutual interest. For example, in 2023, both NSIRA and the National Security and Intelligence Committee of Parliamentarians (NSICOP) launched reviews on the issue of political foreign interference. While maintaining its independence, NSIRA coordinated with NSICOP to avoid any unnecessary duplication of work in relation to each organization's review.

04 //

Reviews

4.1 Overview

43. In addition to its annual reviews, NSIRA continued to execute discretionary reviews that it deemed relevant and appropriate to the authorities of its mandate. Of note was NSIRA's review on the Dissemination of Intelligence on People's Republic of China Political Foreign Interference, 2018–2023. NSIRA evaluated the flow of intelligence within government from the collectors to consumers, including senior public servants and elected officials. This involved scrutinizing internal processes regarding how collected information was shared and escalated to relevant decision-makers. NSIRA determined that it was in the public interest to report on this matter and produced its first special report under section 40 of the NSIRA Act. This report was tabled in both houses of Parliament in May 2024.

44. Table 1 captures all review work that was underway in 2023. This includes annually mandated reviews, discretionary reviews, and annual reviews of CSE and CSIS activities. High-level summaries of their content and outcomes are provided in subsequent sections for those reviews completed by the end of the calendar year; the full findings and recommendations can be found in Annex B. NSIRA makes the reviews available once they have been redacted for public release.

Table 1. NSIRA review activities during 2023

Review	Department(s)	Status*
Annual Report to the Minister of National Defence on CSE activities for 2022	CSE	Completed
Annual Report to the Minister of Public Safety on CSIS activities for 2022	CSIS	Completed
Review of Government of Canada Institutions' Disclosures of Information Under the *Security of Canada Information Disclosure Act* in 2022	Public Safety Canada (PS), CSE, CSIS, GAC, RCMP, and Immigrations, Refugees and Citizenship Canada (IRCC)	Completed
Review of CSE's Network-based solutions and related Cybersecurity & Information Assurance activities	CSE and SSC	Completed

Review	Department(s)	Status*
Review of CSIS Dataset Regime	CSIS	Completed
Review of the Department of National Defence/Canadian Armed Forces' Human Source Handling Program	DND/CAF	Completed
Review of Operational Collaboration between the Communications Security Establishment and the Canadian Security Intelligence Service	CSE and CSIS	Completed
Review of the CBSA's Confidential Human Source Program	CBSA	Completed
Review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2022	CBSA, Canada Revenue Agency (CRA), CSE, CSIS, Department of Fisheries and Oceans (DFO), DND/CAF, Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), GAC, IRCC, PS, RCMP, and Transport Canada (TC)	Completed
CSE's Use of the Polygraph for Security Screening	CSE and TBS	Completed
Review of the dissemination of intelligence on People's Republic of China political foreign interference, 2018–2023	CSIS, RCMP, GAC, CSE, PS, and Privy Council Office (PCO)	Completed
Review of Public Safety Canada and the Canadian Security Intelligence Service's Accountability Mechanisms	CSIS, GAC, PS, and Department of Justice Canada (DOJ)	Completed
Review of the Lifecycle of CSIS' Warranted Information	CSIS	Completed
Review of the RCMP's Human Source Program	RCMP	Completed
Review of Government of Canada Institutions' Disclosures of Information Under the *Security of Canada Information Disclosure Act* in 2023	PS, CSE, CSIS, GAC, RCMP, CBSA, and IRCC	Ongoing
Review of CSE's Vulnerabilities Equities Process	CSE, CSIS, and RCMP	Ongoing

Review	Department(s)	Status*
Review of CRA's Review and Analysis Division (RAD)	CRA	Ongoing

*Status as of the writing of this report. A review is marked as "completed" when the review report has been approved by NSIRA members. Reviews listed as "ongoing" may have been completed since the writing of this report and may be available on NSIRA's website.

4.2 Canadian Security Intelligence Service reviews

Overview

45. NSIRA has a mandate to review any Canadian Security Intelligence Service (CSIS) activity. The NSIRA Act requires the agency to submit an annual report on CSIS activities each year to the Minister of Public Safety and Emergency Preparedness[9]. These reports are classified and include information related to CSIS's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of CSIS exercising its powers.

46. In 2023, NSIRA completed one dedicated review of CSIS and its annual review of CSIS activities, both summarized below. Furthermore, CSIS is involved in other NSIRA multi-departmental reviews, such as the agency's review of the operational collaboration between CSE and CSIS, and the legally mandated annual reviews of the *Security of Canada Information Disclosure Act* (SCIDA) and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, the results of which are described in section 4.5, Multi-departmental reviews.

Review of CSIS Dataset Regime

47. In July 2019, the dataset regime came into force as part of the *National Security Act 2017* (NSA 2017*),* creating sections 11.01–11.25 of the CSIS Act. The regime enables CSIS to collect and retain datasets containing personal information that are not directly and immediately related to threats, but likely to assist in national security investigations.

48. NSIRA examined the implementation of the regime, including aspects of governance, information management, retention practices, and training. The agency found compliance issues that permeated all aspects of the regime under review. Of concern, NSIRA found that

[9] With these responsibilities now divided into two portfolios, NSIRA submits its reports to the Minister of Public Safety.

CSIS's current application of the dataset regime is inconsistent with the statutory framework. NSIRA also found multiple compliance issues with how CSIS has implemented the regime, including the retention of Canadian and foreign information without the requisite legally mandated authorizations and approvals.

49. The review concluded that CSIS has failed to adequately operationalize its dataset regime. CSIS did not seek to clarify legal ambiguities of the application of the regime before the Federal Court, despite having had the opportunity to do so. CSIS adopted multiple positions on its application and now risks limiting what is intended to be a collection and retention regime to a retention mechanism. Internally, CSIS has not provided sufficient resources and training to ensure compliance with the regime. Absent an internal commitment to adequately operationalize, resource, and support the implementation of a new legal regime, any such regime will fail no matter how fit for purpose it is believed to be.

Annual review of Canadian Security Intelligence Service activities

50. NSIRA completed its annual review of CSIS activities, which covers a range of activities contemplated and undertaken between January 1 and December 31, 2023. The review highlighted compliance-related challenges faced by CSIS, allowed NSIRA to continue monitoring ongoing trends, and identified emerging issues in CSIS's exercise of its powers. Information obtained throughout the review, including that which CSIS is required to provide to NSIRA under the CSIS Act, was used in NSIRA's Annual Report to the Minister of Public Safety on CSIS activities, as well as to inform ongoing NSIRA reviews and internal review planning for upcoming reviews.

Statistics and data

51. To achieve greater public accountability, NSIRA has requested that CSIS publish statistics and data about public interest and compliance-related aspects of its activities. NSIRA is of the opinion that the following statistics will provide the public with information related to the scope and breadth of CSIS operations, as well as display the evolution of activities from year to year.

Warrant applications

52. Section 21 of the CSIS Act authorizes CSIS to apply to a judge for a warrant if it believes, on reasonable grounds, that more intrusive powers are required to investigate a particular threat to the security of Canada. Warrants may be used by CSIS, for example, to intercept

communications, enter a location, or obtain information, records, or documents. Each individual warrant application could include multiple individuals or request the use of multiple intrusive powers.

Table 2: Section 21 warrant applications made by the Canadian Security Intelligence Service, 2018–2023

Applications	2018	2019	2020	2021	2022*	2023
Total section 21 applications	24	24	15	31	28	30
Total approved warrants	24	23	15	31	28	30
New warrants	10	9	2	13	6	9
Replacements	11	12	8	14	14	10
Supplemental	3	2	5	4	8	11
Total denied warrants	0	1	0	0	0	0

*The applications submitted by CSIS to the Federal Court in 2022 resulted in the approval and issuance of 194 judicial authorities, including 164 warrants and 28 assistance orders issued pursuant to sections 12, 16, and 21 of the CSIS Act, as well as two judicial authorizations issued pursuant to section 11.13 of the Act. Each application is subject to a thorough production and vetting process that includes review by an independent Department of Justice counsel and challenge by a committee composed of executives of CSIS, PS, CSE, and the RCMP (as applicable) before seeking ministerial approval. A number of warrants issued during this period reflected the development of innovative new authorities and collection techniques, which required close collaboration between collectors, technology operators, policy analysts, and legal counsel.

Threat reduction measures

53. CSIS is authorized to seek a judicial warrant for a threat reduction measure (TRM) if it believes that certain intrusive measures, outlined in section 21 (1.1) of the CSIS Act, are required to reduce a threat. The CSIS Act is clear that when a proposed TRM would limit a right or freedom protected by the *Canadian Charter of Rights and Freedoms* or would otherwise be contrary to Canadian law, a judicial warrant authorizing the measure is required. To date, CSIS has sought no judicial authorizations to undertake warranted TRMs. TRMs approved in one year may be executed in future years. Operational reasons may also prevent an approved TRM from being executed.

Table 3: Total number of approved and executed threat reduction measures, 2015–2023

Threat reduction measures	2015	2016	2017	2018	2019	2020	2021	2022	2023
Approved	10	8	15	23	24	11	23	16	14
Executed	10	8	13	17	19	8	17	12	19
Warranted	0	0	0	0	0	0	0	0	0

Canadian Security Intelligence Service targets

54. CSIS is mandated to investigate threats to the security of Canada, including espionage; foreign-influenced activities; political, religious, or ideologically motivated violence; and subversion.[10] Section 12 of the CSIS Act sets out criteria for permitting the Service to investigate an individual, group, or entity for matters related to these threats. Subjects of a CSIS investigation, whether they be individuals or groups, are called "targets."[11]

Table 4: Number of Canadian Security Intelligence Service targets, 2018–2023

Targets	2018	2019	2020	2021	2022	2023
Number of targets	430	467	360	352	340	323

Datasets

55. Data analytics is an investigative tool for CSIS, through which it seeks to make connections and identify trends that may not be visible using traditional methods of investigation. NSA 2017 gave CSIS new powers, including a legal framework for the Service to collect, retain, and use datasets. The framework authorizes CSIS to collect datasets (divided into publicly available, Canadian, and foreign datasets) that may have the ability to assist it in the performance of its duties and functions. It also establishes safeguards for the protection of Canadian rights and freedoms, including privacy rights. These protections include enhanced requirements for

[10] The CSIS Act, section 2, defines threats to national security.
[11] See the *Report of the Events Related to Maher Arar*, Factual Background Volume I, note 10.

ministerial accountability. Depending on the type of dataset, CSIS must meet different requirements before it is able to use a dataset.[12]

56. The CSIS Act also requires that NSIRA be kept apprised of certain dataset-related activities. Reports prepared following the handling of datasets are to be provided to NSIRA under certain conditions and within reasonable timeframes. While CSIS is not required to advise NSIRA of judicial authorizations or ministerial approvals for the collection of Canadian and foreign datasets, CSIS has been proactively keeping NSIRA apprised of these activities.

Table 5: Evaluation and retention of publicly available, Canadian, and foreign datasets by the Canadian Security Intelligence Service, 2019–2023

Type of dataset	2019	2020	2021	2022	2023
Publicly available					
Evaluated	9	6	4	4	2
Retained	9	6	2[a]	4	2
Canadian					
Evaluated	0	0	2	0	1
Retained (approved by the Federal Court)	0	0	0	2[b]	0
Denied by the Federal Court	0	0	0	0	0
Foreign					
Evaluated	10	0	0	1	2
Retained (approved by the Minister of Public Safety and Intelligence Commissioner)	0	1	1[c]	1	3
Denied by the Minister	0	0	0	0	0
Denied by the Intelligence Commissioner	0	0	0	0	0

[12] Amendments to the CSIS Act – Data Analytics Backgrounder. CSIS. (July 18, 2020).

Note: The statistics reported in this table are current as of May 2024. Statistics from previous annual reports have been updated to reflect new data received.
[a] In 2021, CSIS evaluated four publicly available datasets. It retained two, and of the other two, found that one had been sent late for evaluation (and so was deleted with no information retained) and the other was found to be administrative (and not subject to section 11 of the CSIS Act).
[b] Datasets collected and evaluated in 2021 received judicial authorization, and were therefore retained in 2022.
[c] In 2019, CSIS sought ministerial authorization to retain ten foreign datasets. While no foreign datasets were evaluated in 2020 or 2021, one foreign dataset was retained following ministerial authorization (by the Director as designate) and ratification by the Intelligence Commissioner, further to an application made in 2019.

Justification Framework

57. CSIS's Justification Framework establishes a limited justification for its employees, and persons acting at their direction, to carry out activities that would otherwise constitute offences under Canadian law. CSIS's framework is modelled on those already in place for Canadian law enforcement.[13] It provides needed clarity to CSIS, and to Canadians, about what CSIS may lawfully do in the course of its activities. The framework recognizes that it is in the public interest to ensure that CSIS employees can effectively carry out intelligence collection duties and functions, including by engaging in otherwise unlawful acts or omissions, in the public interest and in accordance with the rule of law. The types of otherwise unlawful acts and omissions that are authorized by the Justification Framework are determined by the Minister of Public Safety and approved by the Intelligence Commissioner. There remain limitations on what activities can be undertaken, and nothing in the framework permits the commission of an act or omission that would infringe on a right or freedom guaranteed by the Charter.

58. According to section 20.1 of the CSIS Act, employees must be designated by the Minister of Public Safety and Emergency Preparedness to be covered under the Justification Framework while committing or directing an otherwise unlawful act or omission. Designated employees are CSIS employees who require the Justification Framework as part of their duties and functions. Designated employees are justified in committing an act or omission themselves (commissions by employees) and they may direct another person to commit an act or omission (directions to commit) as a part of their duties and functions.

[13] See https://www.canada.ca/en/security-intelligence-service/news/2020/06/amendments-to-the-csis-act--justification-framework.html.

Table 6: Authorizations, commissions, and directions under CSIS' Justification Framework, 2019–2023

	2019	2020	2021	2022	2023
Authorizations	49	147	178	172	172
Commissions by employees	1	39	51	61	47
Directions to commit	15	84	116	131	116
Emergency designations	0	0	0	0	0

Note: The statistics reported in this table are current as of May 2024. Statistics from previous annual reports have been updated to reflect new data received.

Compliance

59. CSIS's operational compliance program unit leads and manages overall compliance within the Service. The objective of this unit is to promote a culture of compliance within CSIS by leading an approach for reporting and assessing potential non-compliance incidents that provides timely advice and guidance related to internal policies and procedures for employees. This program is the centre for processing all instances of potential non-compliance related to operational activities.

60. NSIRA will continue to monitor closely the instances of non-compliance that relate to Canadian law and the Charter, and work with CSIS to improve transparency around these activities.

Table 7: Total number of non-compliance incidents processed by CSIS, 2019–2023

Incidents	2019	2020	2021	2022	2023
Processed compliance incidents	53	99	85	59	79
Administrative		53	64	42	48
Operational [a]	40[b]	19[b]	21	17	31
Canadian law	Not available	Not available	1	2	4
Charter	Not available	Not available	6	5	15
Warrant conditions	Not available	Not available	6	3	11
CSIS governance	Not available	Not available	8	15	27

[a] For 2021, each operational non-compliance incident was reported based on the highest non-compliance (i.e., if the incident were non-compliant with the Charter and CSIS governance, it would be counted only under the Charter category). For 2022 and 2023, each incident is counted in all of the areas in which it was non-compliant. As such, the sum of operational non-compliance in the various categories exceeds the total number of such incidents.

[b] The total number of incidents of non-compliance were not further broken down in 2019 and 2020. This number represents the number of incidents of non-compliance with requirements such as the CSIS Act, the Charter, warrant terms and conditions, or CSIS internal policies or procedures.

4.3 Communications Security Establishment reviews

Overview

61. NSIRA has the mandate to review any activity conducted by the Communications Security Establishment (CSE). NSIRA must submit an annual report to the Minister of National Defence on CSE activities, including information related to CSE's compliance with the law and applicable ministerial directions, and NSIRA's assessment of the reasonableness and necessity of CSE exercising its powers.

62. In 2023, NSIRA completed two dedicated reviews of CSE and commenced an annual review of CSE activities, summarized below. Furthermore, CSE is included in other NSIRA multi-

departmental reviews, such as the review of the operational collaboration between CSE and CSIS and the legally mandated annual reviews of the *Security of Canada Information Disclosure Act* (SCIDA) and the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (see section 4.5).

Review of CSE's Use of the Polygraph for Security Screening

63. NSIRA's review of CSE's use of the polygraph for security screening found that the policies and procedures in place at CSE inadequately addressed privacy issues. In particular, CSE's use of personal information collected during polygraph exams for staffing purposes may have exceeded the consent provided and may not have complied with section 7 of the *Privacy Act*.

64. NSIRA also found issues with the way in which CSE operated its polygraph program, including unnecessarily repetitive and aggressive questioning by examiners, insufficient quality control of exams, and retention issues related to audiovisual recordings. Additionally, the way in which CSE used the results of polygraph exams to inform security screening decision-making could cause uncertainty over the opportunity to challenge denials of security clearances pursuant to the NSIRA Act. CSE generally over-relied on the results of polygraph exams for deciding security screening cases. When taken as a whole, CSE's use of the polygraph for security screening raised serious concerns related to the Charter.

65. NSIRA also explored the role of the Treasury Board of Canada Secretariat (TBS) in establishing the Standard on Security Screening (the Standard), which governs the use of the polygraph for security screening by the Government of Canada. NSIRA found that TBS did not adequately consider the privacy or Charter implications of the use of the polygraph. TBS also did not implement sufficient safeguards in the Standard to address these implications.

66. As a result, NSIRA recommended that CSE and TBS both urgently address the fundamental issues related to the legality, reasonableness, and necessity of the use of the polygraph for security screening. If these issues cannot be addressed, NSIRA recommended that TBS remove the polygraph from the Standard and CSE should cease using it for security screening.

Review of CSE's Network-based solutions and related Cybersecurity & Information Assurance activities

67. Since the CSE Act came into force in 2019, CSE's cybersecurity and information assurance (CSIA) activities have grown in extent and importance. CSE acquires and analyzes vast amounts

of information to identify and prevent cybersecurity threats, a necessary activity that nonetheless engages important privacy interests, a balance NSIRA sought to understand.

68. This was NSIRA's first review of CSE's CSIA activities, along with its first review of Shared Services Canada (SSC). The two departments work together on CSIA activities, as SSC is the system owner for most Government of Canada networks.

69. NSIRA found that CSE operates a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities to protect against cyber threats, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

70. NSIRA made findings and recommendations in two areas of concern:

    - CSE's communications to the Minister of National Defence about its CSIA program did not fully reflect its activities in practice. NSIRA made recommendations to CSE to improve its transparency in this regard.

    - CSE acquired information from sources that, in limited cases, may engage Canadian privacy interests. While this information has clear cybersecurity value, it was not acquired within the scheme of ministerial authorizations, due in part to an incongruence between subsections of the CSE Act. NSIRA recommended various actions to address this acquisition.

71. NSIRA built foundational knowledge about CSE's CSIA activities through this review, which will inform NSIRA's future activities.

Annual review of Communications Security Establishment activities

72. NSIRA conducted the second annual review of CSE activities. The 2023 review aimed to identify compliance-related challenges, general trends, and emerging issues based on information CSE is required by law to provide to NSIRA, as well as supplementary information. Primarily resulting in NSIRA's Annual Report to the Minister of National Defence on CSE activities, the review also identified areas for future reviews of CSE activities and bolstered NSIRA's knowledge of CSE activities.

Statistics and data

73. To achieve greater accountability and transparency, NSIRA has requested statistics and data from CSE about public interest and compliance-related aspects of its activities. NSIRA is of the opinion that these statistics will provide the public with important information related to the scope and breadth of CSE operations, as well as display the evolution of activities from year to year.

Ministerial authorizations and ministerial orders

74. Ministerial authorizations are issued to CSE by the Minister of National Defence. The authorizations support specific foreign intelligence, cybersecurity activities, defensive cyber operations, or active cyber operations conducted by CSE pursuant to those aspects of its mandate. Authorizations are issued when these activities could otherwise contravene an Act of Parliament or interfere with a reasonable expectation of privacy of a Canadian or a person in Canada.

Table 8: Ministerial authorizations issued, 2019–2023

Type of ministerial authorization	Enabling section of the CSE Act	Issued in 2019	Issued in 2020	Issued in 2021	Issued in 2022	Issued in 2023
Foreign intelligence	26(1)	3	3	3	3	3
Cybersecurity (federal and non-federal)	27(1) and 27(2)	2	1	2	3	3
Defensive cyber operations	29(1)	1	1	1	1	1
Active cyber operations	30(1)	1	1	2	3	3

Note: This table lists ministerial authorizations that were issued in a given calendar year and may not necessarily reflect ministerial authorizations that were in effect at a given time. For example, if a ministerial authorization was issued in late 2022 and remained in effect in parts of 2023, it is counted solely as a 2022 ministerial authorization.

75. Ministerial orders are issued by the Minister for the purpose of (1) designating any electronic information, any information infrastructures, or any class of electronic information or

information infrastructures as electronic information or information infrastructures of importance to the Government of Canada (section 21[1] of the CSE Act); or (2) designating recipients of information related to Canadians or persons in Canada – that is, Canadian-identifying information (sections 45 and 44[1] of the CSE Act).

Table 9: Ministerial orders in effect as of 2023

Name of ministerial order	Enabling section of the CSE Act
Designating Recipients of Canadian Identifying Information Used, Analyzed or Retained Under a Foreign Intelligence Authorization	43
Designating Recipients of Information Relating to a Canadian or Person in Canada Acquired, Used or Analyzed Under the Cybersecurity and Information Assurance Aspects of the CSE Mandate	44
Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada	21
Designating Electronic Information and Information Infrastructures of Ukraine as of Importance to the Government of Canada	21
Designating Electronic Information and Information Infrastructures of Latvia as of Importance to the Government of Canada	21

Note: Ministerial orders remain in effect until rescinded by the Minister.

Foreign intelligence reporting

76. Under section 16 of the CSE Act, CSE is mandated to acquire information from or through the global information infrastructure. The CSE Act defines the global information infrastructure as including electromagnetic emissions; any equipment producing such emissions; communications systems; information technology systems and networks; and any data or technical information carried on, contained in, or relating to those emissions, that equipment, those systems, or those networks. CSE uses, analyzes, and disseminates the information for providing foreign intelligence in accordance with the Government of Canada's intelligence priorities.

Table 10: Number of foreign intelligence reports issued, 2019–2023

CSE foreign intelligence reporting	2020 (#)	2021 (#)	2022 (#)	2023 (#)
Reports released	Not available	3,050	3,185	3,184
Departments and agencies	>25	28	26	28
Specific clients within departments and agencies	>2,100	1,627	1,761	2,049

Note: NSIRA did not ask CSE for statistics related to foreign intelligence reporting for its 2019 public annual report. In 2020, statistics were requested, but were provided in general terms due to the classification of the data at the time, and CSE indicated that release of further detail would be injurious to national security.

Information relating to a Canadian or a person in Canada

77. Information relating to a Canadian or a person in Canada (IRTC) is information about Canadians or persons in Canada that may be incidentally collected by CSE while conducting foreign intelligence or cybersecurity activities under the authority of a ministerial authorization. Incidental collection refers to information acquired that CSE was not deliberately seeking and where the activity that enabled its acquisition was not directed at a Canadian or a person in Canada. According to CSE policy, IRTC is defined as any information recognized as having reference to a Canadian or person in Canada, regardless of whether that information could be used to identify that Canadian or person in Canada.

78. CSE was asked to release statistics or data about the regularity with which IRTC is included in CSE's end-product reporting. CSE responded that this information "remains classified and cannot be published."

Canadian-identifying information

79. CSE is prohibited from directing its activities at Canadians or persons in Canada. However, its collection methodologies sometimes result in incidentally acquiring such information. When such incidentally collected information is used in CSE's foreign intelligence reporting, any part that potentially identifies a Canadian or a person in Canada is suppressed to protect the privacy of the individual(s) in question. CSE may release unsuppressed Canadian-identifying information (CII) to designated recipients when the recipients have the legal authority and operational justification to receive it, and when it is essential to international affairs, defence, or security (including cyber security).

Table 11: Number of requests for disclosure of Canadian-identifying information, 2021–2023

Type of request	2021 (#)	2022 (#)	2023 (#)
Government of Canada requests	741	657	1,087
Five Eyes requests	90	62	142
Non-Five Eyes requests	0	0	0
Total	831	719	1,229

80. In 2023, of the 1,229 requests received, CSE reported having denied 281 requests. By the end of the calendar year, 40 were still being processed.

81. CSE was asked to release the number of instances where CII is suppressed in CSE foreign intelligence or cyber security reporting. It indicated that this information "remains classified and cannot be published."

Privacy incidents and procedural errors

82. A privacy incident occurs when the privacy of a Canadian or a person in Canada is put at risk in a manner that runs counter to, or is not provided for, in CSE's policies. CSE tracks such incidents through its Privacy Incidents File,[14] and for privacy incidents that are attributable to a second-party partner or a domestic partner, through its Second-Party Privacy Incidents File.

Table 12: Number of privacy incidents recorded by CSE, 2021–2023

Type of incident	2021 (#)	2022 (#)	2023 (#)
Privacy incidents	96	114	107
Second-party privacy incidents	33	23	37
Non-privacy compliance incidents	Not available	Not available	28

[14] As of the fourth quarter of fiscal year 2021–2022, CSE stopped differentiating between the Privacy Incidents File and Minor Procedural Errors File, as incidents in each type fit the same CSE definition of a privacy incident. Procedural errors are now reported within the Privacy Incidents File.

Note: NSIRA did not ask CSE for statistics related to non-privacy compliance incident reporting for its 2021 and 2022 public annual report.

Table 13: Number of privacy incidents that occurred under the foreign intelligence aspect of CSE's mandate and recorded in 2023

Type of incident	2023 (#)
Privacy incidents	70
Second-party privacy incidents	37
Non-privacy compliance incidents	16

Table 14: Number of privacy incidents that occurred under the cybersecurity and information assurance aspect of CSE's mandate and recorded in 2023

Type of incident	2023
Privacy incidents	37
Non-privacy compliance incidents	12

Cyber security and information assurance

83. Under section 17 of the CSE Act, CSE is mandated to provide advice, guidance, and services to help protect electronic information and information infrastructures of federal institutions, as well as those of non-federal entities that are designated by the Minister of National Defence as being of importance to the Government of Canada.

84. The Canadian Centre for Cyber Security (Cyber Centre) is Canada's unified authority on cybersecurity. The Cyber Centre, which is a part of CSE, provides expert guidance, services, and education while working in collaboration with stakeholders in the private and public sectors. The Cyber Centre handles incidents in government and designated institutions that include:

- reconnaissance activity by sophisticated threat actors;
- phishing incidents (email containing malware);
- unauthorized access to corporate IT environments;
- imminent ransomware attacks; and
- zero-day exploits, which involve exploration of critical vulnerabilities in unpatched software.

Table 15: Number of cyber incident cases opened by CSE, 2022 and 2023

Type of cyber incident	2022	2023
Federal institutions	1,070	977
Critical infrastructure	1,575	1,756
International	Not available	82
Total	2,645	2,815

Note: NSIRA did not ask CSE for statistics related to international incident reporting for its 2022 public annual report.

Defensive and active cyber operations

85. Under section 18 of the CSE Act, CSE is mandated to conduct defensive cyber operations (DCO) to help protect electronic information and information infrastructures of federal institutions, as well as those of non-federal entities that are designated by the Minister as being of importance to the Government of Canada, from hostile cyber attacks.

86. Under section 19 of the CSE Act, CSE is mandated to conduct active cyber operations (ACO) against foreign individuals, states, organizations, or terrorist groups as they relate to international affairs, defence, or security.

87. CSE was asked to release the number of DCOs and ACOs approved, and the number carried out in 2023. CSE responded that this information "remains classified and cannot be published."

Technical and operational assistance

88. As part of the assistance aspect of CSE's mandate, CSE receives requests for assistance from Canadian law enforcement and security agencies, as well as from the Department of National Defence and the Canadian Forces (DND/CAF).[15]

[15] CSE was asked to provide the breakdown of requests for assistance by the requesting department but this information could not be shared for publication due to its classification.

Table 16: Number of requests for assistance received and actioned by CSE, 2020–2023

Action	2020	2021	2022	2023
Approved	23	32	59	48
Not approved	1	3	0	0
Under review	Not available	Not available	0	2
Cancelled	Not available	Not available	1	0
Denied	Not available	Not available	2	1
Total received	**24**	**35**	**62**	**53**

Note: For 2020 and 2021, CSE was able to provide only the number of requests received and actioned. CSE advised, however, that it has since improved its internal tracking system for requests for assistance.

4.4 Other department reviews

Overview

89. In addition to the CSIS and CSE reviews above, NSIRA completed the following reviews of departments and agencies in 2023:

- a review of the Canada Border Services Agency (CBSA);
- a review of the Department of National Defence (DND) and the Canadian Armed Forces (CAF); and
- NSIRA's annual reviews of both the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act,* both of which involve a broader set of departments and agencies that make up the Canadian national security and intelligence community.

Canada Border Services Agency

Review of the CBSA's Confidential Human Source Program

90. This review examined the legal and policy frameworks governing CBSA's Confidential Human Source (CHS) program. The review had three areas of focus: the management and assessment of risk; CBSA's discharge of its duty of care to its sources; and the sufficiency of ministerial direction and accountability in relation to the program. Together, these areas support CBSA's ability to conduct its human source-handling activities lawfully, ethically, and with appropriate accountability.

91. The review reflects that, as an investigative tool used in support of CBSA's mandate, the CHS Program rests on an adequate legal framework. However, the review found a number of gaps in the framework governing the program and was especially attentive to how CBSA manages the particular risks associated with the use of human sources without status in Canada. The review contains a number of findings that relate to CBSA's risk management practices.

92. In two instances, NSRIA's review concluded that CBSA's activities may not be in compliance with the law. In the first, the review concluded through a detailed case study that CBSA may have twice breached the law of informer privilege by improperly disclosing information that might identify the human source. In this and another instance, NSIRA found that CBSA failed to inform the Minister of Public Safety of a human source activity that may have impacted the safety of an individual, as required by the Ministerial Direction on Surveillance and Confidential Human Sources. This constitutes non-compliance with subsection 12(2) of the CBSA Act.

93. NSIRA made six recommendations in this review. Collectively, they are meant to enhance the governance of the human source program to ensure CBSA is attentive to the welfare of its human sources across the full spectrum of activities. They also reflect NSIRA's ongoing attention to the principle of ministerial accountability. Overall, NSIRA's findings and recommendations reflect the level of maturity of CBSA's program; although it has been operating for almost 40 years, the introduction of the policy suite specific to human sources is a relatively recent innovation. The review also reflects CBSA's recent efforts to improve its program.

Department of National Defence and the Canadian Armed Forces

Review of DND/CAF's Human Source Handling Program

94. This review examined whether DND/CAF conducts its human source-handling activities lawfully, ethically, and with appropriate accountability.

95. NSIRA found that DND/CAF's policy framework allows human source-handling activities that may not be in compliance with the law. These risks arise particularly in relation to sources associated with terrorist groups. NSIRA recommended that Parliament enact a justification framework that would authorize DND/CAF and its sources to commit otherwise unlawful acts outside Canada, where reasonable for the collection of defence intelligence.

96. NSIRA found that DND/CAF's risk assessment frameworks do not provide commanders with the accurate, consistent, and objective information they need to evaluate the risks of engaging with particular sources. NSIRA recommended that these frameworks be revised to ensure that all applicable risk factors are considered.

97. NSIRA found gaps in DND/CAF's discharge of its duty of care to sources. Safeguarding processes were not always appropriately engaged; the complaints process was underdeveloped; and the risk posed to agents was, at times, insufficiently assessed. Measures to address these issues should be clearly operationalized in governance documents.

98. NSIRA found that the Minister of National Defence is not sufficiently informed on human source-handling operations to fulfill their ministerial accountabilities. The Minister should be aware of the legal, policy, and governance issues that may affect human source-handling operations.

99. NSIRA also found that further ministerial direction is required to support the governance of DND/CAF's human source handling program. NSIRA recommended that the Minister issue ministerial direction to DND/CAF that will guide the lawful and ethical conduct of source-handling operations.

4.5 Multi-departmental reviews

Review of Operational Collaboration between CSE and CSIS

100. CSE and CSIS are two core pillars of Canadian intelligence collection, which means that effective collaboration between the departments is critical to national security. However, a tension exists between CSIS's mandate, which authorizes collection and sharing of information about Canadians, and CSE's core prohibition against directing its activities at Canadians. This is the first review that was able to access information from both departments and consider that tension.

101. NSIRA examined a sample of CSE and CSIS collaborative operational activities and information sharing, as well as collaboration between CSIS and CSE further to CSIS's threat reduction measure (TRM) mandate. This satisfied NSIRA's annual requirement under section 8(2) of the NSIRA Act to review an aspect of CSIS's TRMs.

102. With respect to operational collaboration, including under CSIS's TRM mandate, NSIRA found a lack of information sharing and proactive planning, as well as a failure on CSE's part to properly account for and mitigate the risk of targeting Canadians when working with CSIS. NSIRA recommended some procedural changes to improve information flow, consultation, transparency, and accountability.

103. Concerning information sharing, NSIRA found that existing processes between the departments lacked guidance and accountability, and created risks of CSE targeting Canadians that were actualized in some instances. NSIRA recommended both departments establish policies, procedures, and analyst training. Additionally, NSIRA recommended that CSIS cease making requests to CSE pertaining to Canadians and consider the Canadian information it shares with CSE. NSIRA also recommended that CSE reconsider how it collects, retains, and reports Canadian information in certain scenarios and only use foreign lead information from CSIS reporting.

104. In this review, NSIRA found two cases of non-compliance with the law. Both involved CSE directing its activities at Canadians under its foreign intelligence mandate.

Review of federal institutions' disclosures of information under the *Security of Canada Information Disclosure Act* in 2022

105. This review provided an overview of the use of the *Security of Canada Information Disclosure Act* (SCIDA) in 2022. In doing so, it documented the volume and nature of information disclosures made under the SCIDA, assesses compliance with the Act, and highlights patterns in its use across Government of Canada institutions and over time.

106. In 2022, four disclosing institutions made a total of 173 disclosures to five recipient institutions. NSIRA found that institutions complied with the SCIDA's requirements for disclosure and record keeping in relation to the majority of these disclosures. Observed instances of non-compliance that were related to subsection 9(3), regarding the timeliness of records copied to NSIRA; subsection 5.1(1), regarding the timeliness of destruction or return of personal information; and subsection 5(2), regarding the provision of a statement on accuracy and reliability. These instances did not point to any systemic failures in Government of Canada institutions' implementation of the Act.

107. NSIRA also made findings in relation to practices that, although compliant with the SCIDA, left room for improvement. NSIRA's corresponding recommendations were designed to increase standardization across the Government of Canada in a manner that is consistent with the institutions' demonstrated best practices and the Act's guiding principles.

108. Overall, NSIRA observed improvements in reviewee performance compared to findings from prior years' reports and over the course of the review. These improvements include corrective actions taken by reviewees in response to NSIRA's requests for information in support of this review.

Review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2022

109. This review assessed departments' compliance with the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACA) and their implementation of the ACA's associated directions during the 2022 calendar year. Within this context, the review pursued a thematic focus on departments' conduct of risk assessments, including the ways in which their methodologies may lead to a systematic under-assessment of the level of risk involved in an information-sharing transaction.

110. NSIRA's findings and recommendations in this report reflect both developments and stagnations in departments' implementation of the directions over time. NSIRA observed efforts to collaborate interdepartmentally and standardize certain practices across the Government of Canada. While these efforts reflect an improvement over past approaches, they fall short of the consistent framework for foreign information sharing government-wide envisioned by the Act. Additionally, NSIRA observed a number of practices that may lead departments to systematically under-assess the risks involved in contemplated information exchanges. Such under-assessments may in turn lead to information being exchanged, in contravention of the directions' prohibitions.

111. NSIRA made five recommendations in this review. Collectively, they would ensure that all departments' ACA frameworks reflect a degree of standardization commensurate with the spirit of the Act and its associated directions; and that these frameworks are designed to support compliance with the directions.

05 //

Complaint investigations

5.1 Overview

112. NSIRA is mandated to investigate national security-related public complaints. NSIRA complaint investigations are conducted with consistency, fairness, and timeliness. The agency's public complaint mandate plays a critical role in ensuring that Canada's national security and intelligence organizations are accountable to the Canadian public.

113. In 2022, NSIRA had committed to establishing service standards for the investigation of complaints, with the goal of completing 90 percent of investigations within its new service standards. These service standards were implemented and have been in effect since April 1, 2023, and set internal time limits for certain investigative steps for each type of complaint, under normal circumstances. NSIRA is pleased to report that for the period of April 1 to December 31, 2023, 100 percent of the service standards have been met across all investigation files subject to these service standards.

114. While remaining mindful of the interests of the complainant and the security imperatives of the organization, NSIRA established an independent verification process with CSE for new complaints filed under section 17 of the NSIRA Act. More specifically, after receiving a complaint, NSIRA must evaluate whether it is within NSIRA's jurisdiction to investigate, based on conditions stated in the NSIRA Act. For complaints against CSE, just as with complaints against CSIS and the RCMP, NSIRA must be satisfied that the complaint against the respondent organization refers to an activity carried out by the organization and is not trivial, frivolous, or vexatious. This new independent verification process assists NSIRA in ascertaining its jurisdiction to investigate complaints filed against CSE.

115. NSIRA has developed a new internal tracking tool to ensure effective case management of complaint files.

116. NSIRA previously reported that it would improve its website to promote accessibility to the investigation of complaints. During the overhaul of its public-facing website in the fall of 2023, NSIRA amended its complaint forms to ensure that they meet WCAG 2.0 accessibility criteria and conformity requirements.

117. In 2023, NSIRA completed the last phase of a study jointly commissioned with the Civilian Review and Complaints Commission (CRCC) regarding the collection of race-based data and other demographic information. The study assessed the viability of the collection of identity-based and demographic data as part of the Government of Canada's ongoing anti-racism initiatives.

118. In the course of this study, interviews were conducted with community members familiar with NSIRA, the CRCC, and the agencies they review. The study ultimately found that the collection of raced-based data was feasible.

119. The study also included recommendations in relation to the collection of race-based data as follows:

- collection of race data from complainants and how to collect such data;
- collection of other biographical data from complainants;
- collection of race data about the staff police and intelligence organizations;
- analysis of the collected data;
- provision of the collected data to interested stakeholders, the general public, or both;
- development of an advanced data analysis plan.

120. NSIRA welcomes the insights provided by the joint study and will closely review the recommendations to determine how they might be implemented by NSIRA. The collection of race-based and other demographic data in the national security and intelligence space is an entirely novel area. The study's literature review highlighted that this type of race-based and other demographic data collection has never been done before in the national security and intelligence space in Canada, or by any of Canada's international partners. NSIRA and the CRCC will continue to collaborate on this important initiative by determining potential implementation strategies.

5.2 Ongoing initiatives

121. In 2023, NSIRA began revising its *Rules of Procedure* to refine the procedures governing its complaints investigations. This revision will continue in 2024 with the support of the Secretariat in ensuring that the agency's obligations provided for in its *Accessibility Plan* are met.

122. Part of the revisions to NSIRA's procedures in 2024 will be to review the privacy statement included in its complaint forms to ensure greater transparency about how the information submitted to NSIRA by complainants will be used in NSIRA's investigations.

5.3 Investigation summaries

Final reports issued

Investigation concerning allegations against CSIS (NSIRA File 07-403-45)

123. The complainant alleged that CSIS agents interacted with them on multiple occasions and claimed that those interactions amounted to illegal arrests and detentions; that the agents illegally intimidated them by claiming that they would deport them to Guantanamo Bay; and that the Service erroneously applied the *Privacy Act* in refusing to provide documents the complainant claims they were coerced into signing under duress during one of the above-noted interactions.

124. Upon reviewing all of the evidence presented by the parties and available information, NSIRA observed that the complainant never had any interactions with CSIS. NSIRA found that none of their allegations could be substantiated.

Allegations against CSIS for travel difficulties, harassment, and discrimination (NSIRA File 07-403-23)

125. The complainant alleged that, following an overseas trip, they experienced difficulties travelling internationally, which they believed were attributable to CSIS and CSIS' sharing of information with the governments of foreign countries. The complainant claimed that CSIS had placed them on a "blacklist" as a member of the Islamic State of Iraq and Syria. They further alleged that CSIS harassed them and discriminated against them on the basis of race, ethnic origin, and religion.

126. At the time of the complainant's trip, certain countries were regularly being used by extremist travellers from North America and Europe as intermediate destinations to access Islamic State of Iraq and the Levant-controlled territory.

127. The complainant's family was interviewed by CSIS to gain information about the complainant, their beliefs, and possible intentions. The complainant considered this interaction to have been an inappropriate and wrongful interrogation of members of their family.

128. Upon review of all of the evidence, NSIRA found the activities of CSIS in this matter to have been lawful and reasonable. While investigative steps were conducted by CSIS, there was no evidence suggesting that CSIS placed the complainant on a blacklist or that information pertaining to the complainant was shared improperly. Similarly, the allegation that CSIS was responsible for the complainant's travel difficulties was found to be unsubstantiated. The source of the complainant's travel difficulties may lie outside of Canadian authorities, and thus beyond the scope of NSIRA's jurisdiction.

129. NSIRA concluded that CSIS conducted an interview with the complainant's parent at their home and with other family members present, during which their parent participated voluntarily and expressed their willingness to be of further assistance if required. The basis for conducting this interview was found to be reasonable and NSIRA did not find any evidence of inappropriateness, intimidation, wrongdoing, or harassment.

130. NSIRA did not find an evidentiary basis to support the allegations of harassment and of discrimination on the basis of racial, ethnic origins, or religion by CSIS against the complainant.

131. The complainant's allegations were found to be unsupported.

Allegations against CSIS regarding criminal activity conducted by a CSIS Agent (NSIRA File 07-403-39)

132. The complainant alleged that a CSIS agent invaded their house and stated that they were an intelligence officer in operation. According to the complainant, the CSIS agent physically assaulted them, video recorded the complainant while the complainant was undressed, and threatened to kill them. The complainant further alleged that the Service is trying to silence them.

133. Upon a review of all of the evidence, it became clear that the complainant's own conduct brought them to the attention of CSIS. They first communicated with CSIS and raised complaints regarding an individual. These allegations were received and considered by CSIS, which acted on the complaints to determine whether the individual named by the complainant was affiliated with CSIS. Based on a review of the documents submitted by CSIS, NSIRA determined that the individual alleged by the complainant to be a CSIS Agent was not a CSIS employee or otherwise involved with CSIS.

134. NSIRA further found that as part of the Service's activities conducted in relation to the complainant, CSIS collected limited information on the complainant. NSIRA concluded that the collection of the complainant's personal information was justified by CSIS' mandate.

135. NSIRA concluded that the CSIS' activities in relation to the complainant after they came to their attention were lawful and reasonable in the circumstances.

Allegations against CSIS regarding a citizenship security screening interview (NSIRA File 07-403-65)

136. The complainant had applied for Canadian citizenship and was subsequently required to attend an interview with CSIS. The complainant attended this interview with their lawyer. The complainant alleged that the CSIS officers who conducted the interview:

- denied them and their lawyer the right to record and take notes of the interview;
- violated past SIRC recommendations by not recording the interview themselves;
- interacted with the complainant's lawyer in an intimidating manner, and did not allow the lawyer to interject or to interrupt;
- did not provide an adequate translation service; and
- lacked cultural sensitivity during the interview, used inappropriate interview tactics, chose discussion points that created unnecessary tension, and behaved improperly.

137. Upon considering all of the evidence, NSIRA found that the CSIS officers erred in denying the complainant and their counsel the opportunity to take notes that they could take from the premises. CSIS acknowledged that this practice was no longer in place. NSIRA recommended that CSIS adjust its governing policy to make clear that the interviewee and their representative may take and retain notes from interviews.

138. NSIRA commented that since 2000, numerous SIRC reports and decisions have recommended that CSIS record immigration security screening interviews. However, CSIS did not consistently record such interviews at the time of the complainant's interview. CSIS indicated that efforts to require recording of all immigration interviews in its written procedures was in progress. NSIRA recommended that CSIS proactively record interviews in immigration and citizenship matters, and that CSIS retain this recording at least until a decision is made by Immigration, Refugees and Citizenship Canada (IRCC) on CSIS' advice. In the event that CSIS provides a negative conclusion, the recording should be kept until the immigration status is determined and for the period of any appeal of that determination.

139. Given that the complainant was unable to retain notes from the interview and that no recording of the interview existed, NSIRA was unable to make findings on most of the improper statements that the CSIS interviewer was alleged to have made. However, one statement in

particular, which was an English idiom that the CSIS officer acknowledged using, was found to be unnecessary and counterproductive, as it risked compounding tension in the interview and may not have had a reasonable, literal translation in the language spoken by the complainant.

140. CSIS indicated and NSIRA agreed that counsel to an interviewee has a role in, but not control of, the interview process. An interview subject's lawyer is not limited to passive silence, but also must not act in a manner that impairs the Service's ability to perform its mandate. To this end, it is not open to counsel to lead witnesses or have an intrusive role in questioning. NSIRA noted, however, that it is proper for counsel to raise concerns about interpretation or to suggest clarifying questions. These concerns are to be posed during a pause or in some other pre-organized manner that does not disrupt the questioning. NSIRA recommended, therefore, that CSIS articulate within its own operating procedure the role of counsel (or other third parties) in the manner elaborated above, and that it communicates these expectations in advance to those attending an interview.

141. Finally, to remedy these errors, NSIRA recommended that CSIS convene a second interview attended by different officers and a different interpreter. Given the irregularities in the first interview and the resulting concern that it may contain inaccuracies, NSIRA further recommended that in completing its assessment and in providing advice to the IRCC, CSIS avoid giving weight to the results of the first interview.

Allegations against the RCMP for failure to return seized items (NSIRA File 07-407-08)

142. The complainant filed a complaint against the RCMP alleging that it failed to return property that was seized from their office, resulting from an RCMP investigation into a terrorist plot. The complainant further alleged that the RCMP damaged his property.

143. Upon considering the facts and timeline of the RCMP's investigation that resulted in the seizure of the complainant's property, NSIRA found that the property was properly detained, pursuant to the provisions of the Criminal Code and in accordance with RCMP policy.

144. NSIRA further found that there was no evidence that would permit to conclude that the complainant's property was damaged by the RCMP during and after the seizure.

145. The complainant's allegations were found to be unsupported.

Allegation that the RCMP failed to investigate threats against the Complainant and their family made by a foreign government (NSIRA File 07-407-04)

146. The complainant came to Canada as a refugee fleeing violent persecution. As a result of litigation against their former employer, who was linked to the government of a foreign state, the complainant alleged that they had been the victim of death threats from their former employer and government officials of the country from which they had fled. The complainant believed these threats to be credible, as they were often accompanied by contemporaneous details, such as the complainant's clothing during a particular outing and the location they attended. The complainant believed that representatives of the aforementioned government employed at the country's embassy in Canada were assisting in the surveillance of the complainant and their family, including their children while at school.

147. The complainant alleged that the RCMP failed to conduct a complete investigation into incidents involving threats, including death threats, made against the complainant and their family, and that these decisions by the RCMP were improperly influenced by foreign individuals.

148. The evidence provided by the RCMP demonstrated that it took the necessary steps to review the information submitted by the complainant, but determined that there were insufficient grounds for the RCMP to continue their investigation of the foreign influence aspects of the threats. However, the local police force was the police of jurisdiction for investigating the criminal harassment, threats, and safety concerns related to the complainant. The RCMP advised this police force that information collected by the RCMP would be turned over to them, and asked to be notified should the local police force identify someone in Canada working on behalf of a foreign government to threaten or intimidate the complainant. NSIRA found the RCMP's initial investigation to be reasonably thorough and their ultimate decision to be a justifiable exercise of police discretion.

149. Furthermore, there was no evidence before NSIRA to support the complainant's allegation that the RCMP's decision to discontinue their investigation was improperly influenced by foreign individuals.

150. The complainant's allegations were found to be unsupported.

Allegations against the RCMP in relation to the treatment of family members as part of a tactical operation (NSIRA File 07-407-05)

151. The RCMP arrested the complainant at his home on terrorism-related charges. In the course of the operation, the complainant's family members were handcuffed. It was the complainant's

position that this was improper and that the RCMP officers did not utilize their cultural sensitivity training.

152. NSIRA found that:

- The officers securing the complainant's residence and whose conduct gave rise to this complaint were members of other police forces and not RCMP members.
- Given the police had, at the time, reasonable grounds to believe that the premises might have contained unsecured and dangerous weapons, the initial detention of the complainant's family members by using handcuffs was not arbitrary. However, as soon as the officers had control of the scene, the use of handcuffs was no longer appropriate. It followed that the family members were arbitrarily detained within the meaning of section 9 of the Charter.
- Considering the cultural sensitivity briefing that was provided by the RCMP to the investigators taking part in the operation did address the essential consideration, there was no act or omission by the RCMP that raised the risk of culturally insensitive conduct.

153. NSIRA determined that, although the RCMP assumed a general supervisory role over the execution of the operation, they depended on the professionalism of the other police forces in planning and executing a dynamic search. Given that the conduct of the other police officers who participated in the search could not be attributed to the RCMP, no findings or recommendations were made for the RCMP in keeping with NSIRA's jurisdiction.

Other Outcomes

Allegations against CSIS's role in delaying security assessment regarding immigration or citizenship applications (NSIRA Files 07-403-81, 07-403-87, 07-403-100)

154. The complainants filed complaints against CSIS, alleging that the Service caused a significant delay in submitting the security assessment for their immigration or citizenship applications. During the investigations, NSIRA inquired about whether CSIS could provide updates with respect to their involvement in the respective processes. The Service provided letters to NSIRA that could be shared with the complainants advising them that CSIS had completed its assessment in the security screening process. As the complainants' main allegations were in relation to the delay in the security screening, the matters were informally resolved in accordance with Rule 10.10 of NSIRA's *Rules of Procedure* and the files were closed.

Allegations against the CSE regarding the discrimination of an employment applicant (NSIRA File 07-406-07)

155. The complainant filed a section 17 complaint regarding their employment application with CSE. More specifically, upon completing a student term contract with CSE and receiving a verbal offer for a further contract, CSE decided not to renew the complainant's employment. The complainant alleged that this decision from CSE was based on their ethnicity. Despite the Chief of CSE having received a letter of complaint from the complainant, CSE notified NSIRA that its notification letter constituted their first notice of the complaint and requested that the matter be placed in abeyance (on hold). After completing an internal investigation of the complainant's allegations (independent of NSIRA's complaints process), CSE and the complainant began discussions toward a settlement. The parties ultimately reached a settlement and notified NSIRA accordingly. The complaint was informally resolved pursuant to Rule 10 of NSIRA's *Rules of Procedure* prior to NSIRA rendering a decision on its jurisdiction to investigate this matter.

Allegations against the RCMP for failure to investigate a complaint (NSIRA File 07-407-10)

156. This complaint was referred to NSIRA by the Civilian Review and Complaints Commission (CRCC) for the RCMP, pursuant to subsection 45.53(4.1) of the RCMP Act. The complaint alleged that the RCMP failed to investigate individuals allegedly participating in a militia group. NSIRA tried to establish contact with the complainant several times to proceed with its investigation. NSIRA found that reasonable attempts had been made to communicate with the complainant and that the agency had exhausted all options. Accordingly, NSIRA issued reasons that the complaint had been abandoned, as per NSIRA's *Rules of Procedure*. The complaint investigation file was closed.

5.4 Statistics on complaints investigations

157. Investigations progressed at significant levels in 2023 (see Annex C). NSIRA concluded several investigations and issued seven final reports. Additionally, four files were informally resolved in accordance with Rule 10 of NSIRA's *Rules of Procedure*.

158. In 2023, NSIRA observed an increase of complaints against CSIS, pursuant to section 16 of the NSIRA Act, alleging process delays in immigration or citizenship security screening. Of note, under sections 14 and 15 of the CSIS Act, CSIS provides security advice to IRCC and CBSA to guide determinations with respect to whether citizenship or immigration applicants are threats to the security of Canada. While CSIS is committed to performing its security screening

mandate in a timely manner, there is no standard for time allotted. In the 2023 calendar year, out of the six complaints over which NSIRA assumed jurisdiction under section 16 of the NSIRA Act, five pertained to allegations of delays that complainants attributed to CSIS's security screening activities.

06 //

Conclusion

159. The comprehensive reviews and investigations NSIRA conducted in 2023 underscore the agency's dedication to transparency and accountability. This work has provided constructive recommendations to enhance the operational practices and policy frameworks of Canada's important national security and intelligence actors.

160. NSIRA recognizes the persistent and evolving nature of security threats, which necessitates adaptive and proactive approaches by Canada's security and intelligence agencies. NSIRA is likewise committed to continually refining its methodologies, embracing technological advancements, and strengthening its analytical capabilities to keep pace in a rapidly changing world. NSIRA will continue to engage with domestic and international security and intelligence review partners to improve its practices and foster better public understanding of its work and the value it provides.

161. NSIRA is driven by its role as the trusted eyes and ears of Canadians within the otherwise closed domain of national security and intelligence, providing the critical function of enhancing transparency and accountability. NSIRA's vision, mission, and values reflect this commitment and will guide NSIRA's work at it looks to the future.

07 //

Annexes

Annex A: Abbreviations

Abbreviation	Full Name
ACA	Avoiding Complicity in Mistreatment by Foreign Entities Act
ACO	active cyber operations
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CHRC	Canadian Human Rights Commission
CHS	Confidential Human Source (program)
CII	Canadian-identifying information
CRA	Canada Revenue Agency
CRCC	Civilian Review and Complaints Commission for the RCMP
CSE	Communications Security Establishment
CSIA	Cybersecurity and information assurance
CSIS	Canadian Security Intelligence Service
CTIVD Netherlands	Dutch Review Committee on the Intelligence and Security
Cyber Centre	Canadian Centre for Cyber Security
DCO	defensive cyber operations
DFO	Department of Fisheries and Oceans
DND	Department of National Defence
EOS Norway	Norwegian Parliamentary Oversight Committee on Intelligence and Security Services

FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIORC	Five Eyes Intelligence Oversight and Review Committee
GAC	Global Affairs Canada
GC	Government of Canada
HUMINT	Human Intelligence
IC IG US	United States of America's Inspector General of the Intelligence Community
IGIS Australia	Australia's Inspector-General of Intelligence and Security
IGIS New Zealand	New Zealand's Inspector-General of Intelligence and Security
IPCO UK	United Kingdom's Investigatory Powers Commissioner's Office
IRCC	Immigration, Refugees and Citizenship Canada
IRTC	information relating to a Canadian or a person in Canada
IT	information technology
MD	Ministerial Direction
NBS	network-based solutions
NDA	National Defence Act
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
OA-IA	Independent Oversight Authority for Intelligence Activities of Switzerland
PCLOB US	United States Privacy and Civil Liberties Oversight Board
PCO	Privy Council Office
PKGr	German Parliamentary Oversight Panel
PS	Public Safety Canada
RAD	Review and Analysis Division
RCMP	Royal Canadian Mounted Police
REP	reasonable expectation of privacy

SCIDA	Security of Canada Information Disclosure Act
SIRC	Security and Intelligence Review Committee
SSC	Shared Services Canada
TBS	Treasury Board of Canada Secretariat
TC	Transport Canada
TET Denmark	Danish Intelligence Oversight Board
the Standard	Standard on Security Screening
TRM	threat reduction measure
UNCTED	United Nations' Counter-Terrorism Executive Directorate

Annex B: Review findings and recommendations

This Annex lists the full findings and recommendations of NSIRA's reviews that were completed in 2023. In certain instances, original language has been redacted and replaced with summary language designated by [*summary*]. Once redacted, full reviews and available government responses to recommendations are published on NSIRA's website.

Canadian Security Intelligence Service review

Review of CSIS Dataset Regime[16]

NSIRA's findings

1. NSIRA found that CSIS's current application of the dataset regime is inconsistent with the statutory framework.

2. NSIRA found that CSIS's current approach to dataset information collection under section 12 risks the creation of a parallel collection mechanism, one that weakens section 12's statutory thresholds and at the same time lacks the external oversight regime intended to protect personal information under the dataset regime.

3. NSIRA found that CSIS failed to fully apprise the Court on their interpretation and application of the dataset regime. CSIS should have sought clarification from the Court as to its views on the precise conduct permissible prior to invocating the dataset regime.

4. NSIRA found that when conducting queries in exigent circumstances, CSIS retained information that did not meet the section 12 strictly necessary threshold.

5. NSIRA found that the lack of explicit time limits in section 11.17 of the dataset provisions governing foreign datasets has resulted in datasets being retained for multiple years pending a decision by the Minister or Minister's designate (the CSIS Director).

6. NSIRA found that CSIS runs the risk of collecting information that is publicly available but for which there may be a reasonable expectation of privacy.

[16] See full redacted review : https://nsira-ossnr.gc.ca/en/reviews/ongoing-and-completed-reviews/completed-reviews/nsira-review-of-csis-dataset-regime/

7. NSIRA found that CSIS's policies governing the collection and retention of Canadian and foreign datasets do not align with its current interpretation of the dataset regime.

8. NSIRA found that CSIS does not have a policy governing the handling of transitory information. In addition, the existing *Interim Direction* [***] does not provide employees with sufficient instruction, which may result in CSIS retaining information that would otherwise be subject to the dataset regime.

9. NSIRA found that CSIS information management practices are responsible for multiple compliance incidents and currently create duplicates of datasets within CSIS's systems.

10. NSIRA found that, as of August 2023, CSIS did not comply with the dataset provisions in the CSIS Act because it retained Canadian information extracted from foreign datasets, and foreign information amounting to a dataset.

11. NSIRA found that CSIS did not comply with the dataset provisions in the CSIS Act because it retained Canadian information and referenced it as recently as 2022. This information should have been destroyed upon coming into force of the NSA 2017, in July 2019.

12. NSIRA found that CSIS has not exhaustively scanned all of its systems to identify information that is subject to the dataset regime so that it may be processed in a compliant manner.

13. NSIRA found that the training required to become a designated employee to evaluate, query, and exploit section 11.01 datasets offers clear information on the collection and retention requirements.

14. NSIRA found that CSIS operational personnel, including those predominantly dealing with bulk information collection, have not received adequate training allowing them to identify when collected information may fall within the dataset regime.

15. NSIRA found that CSIS has not prioritized resourcing the technical unit responsible for the evaluation, querying, and exploitation of Canadian and foreign datasets.

16. NSIRA found that CSIS has not devoted sufficient resources to improving the current technical systems or developing new ones that are equipped to support bulk data use.

17. NSIRA found that CSIS collected information in relation to activities that could not on reasonable grounds be suspected to have constituted a threat to the security of Canada and the collection, analysis, and retention of which was not strictly necessary.

NSIRA's recommendations
Recommendation 1: NSIRA recommends that in the next judicial authorization application for a Canadian dataset CSIS put its current position on the application of the dataset regime before the Court, including any use of the information prior to the decision to retain under the dataset regime.
Recommendation 2: NSIRA recommends that CSIS immediately destroy any record containing names retained pursuant to the exigent circumstances queries, as they do not meet the strictly necessary threshold.
Recommendation 3: NSIRA recommends that Parliament legislates a time limitation for the authorization of a foreign dataset by the Minister or Minister's designate.
Recommendation 4: NSIRA recommends that CSIS meaningfully analyze and document any possible reasonable expectation of privacy when evaluating publicly available datasets.
Recommendation 5: NSIRA recommends that CSIS develop: • Guidelines regarding the implementation of section 6 of the Interim Direction on [**redacted**] that also include consideration of how the Direction's retention rule is to be reconciled with the 90 day evaluation period in the dataset regime; and • A policy governing the handling of transitory information.
Recommendation 6: NSIRA recommends that CSIS cease to create duplicates of the information reported in the operational system.
Recommendation 7: NSIRA recommends that CSIS immediately destroy Canadian and foreign dataset information that is not strictly necessary to retain. This information no longer falls within the legal 90 day evaluation period and retaining it pursuant to the dataset regime is no longer a possibility.
Recommendation 8: NSIRA recommends that CSIS conduct an exhaustive scan of its operational and corporate repositories to identify and destroy any non-compliant information.
Recommendation 9: NSIRA recommends that CSIS develop and deliver scenario-based workshops to train operational personnel on CSIS's current application of the dataset regime so that they can engage subject matter experts as necessary.
Recommendation 10: NSIRA recommends that CSIS prioritize resourcing the technical unit responsible for the evaluation, querying, and exploitation of Canadian and foreign datasets.
Recommendation 11: NSIRA recommends that CSIS prioritize the improvement of current technical systems or development of new systems, equipped to support compliant bulk data use.

Recommendation 12: NSIRA recommends that CSIS immediately destroy the case study dataset it collected pursuant to section 12, as it does not meet the statutory thresholds. This information no longer falls within the legal 90 day evaluation period and retaining it pursuant to the dataset regime is no longer a possibility.

Recommendation 13: NSIRA recommends that CSIS share the full unredacted copy of this report with the Federal Court.

Communications Security Establishment reviews

Review of CSE's Use of the Polygraph in Security Screening

NSIRA's findings

1. NSIRA found that CSE's governance of the use of the polygraph for security screening inadequately addresses privacy issues.

2. NSIRA found that CSE did not conduct a Privacy Impact Assessment related to its use of the polygraph for security screening.

3. NSIRA found that CSE may not have considered whether all information collected during the polygraph is directly related or necessary to the assessment of loyalty to Canada or criminality, as required by the *Privacy Act* and the Directive on Privacy Practices.

4. NSIRA found that polygraph examiners applied an ad hoc approach as they assessed medical information collected during the polygraph.

5. NSIRA found that CSE may not have complied with section 7 of the *Privacy Act* by using information collected during polygraph exams for suitability and hiring decisions without the consent of the subject.

6. NSIRA found that CSE provides subjects with information that overstates the reliability and validity of the polygraph prior to obtaining consent.

7. NSIRA found that, in some instances, the way in which CSE conducted polygraph exams risked prompting subjects to fabricate information in an effort to clear themselves when faced with an unfavourable polygraph assessment.

8. NSIRA found instances where CSE's quality control practices for polygraph exams were not always consistent with CSE policy.

9. NSIRA found that approximately 20% of security files from the sample reviewed were missing audiovisual recordings of polygraph exams.

10. NSIRA found that in all cases, when initial polygraph exam results indicated deception or were inconclusive, CSE's practice was to conduct multiple polygraph exams rather than a resolution of doubt process as provided for under the Standard.

11. NSIRA found that the polygraph had an inordinate importance in security screening decision-making at CSE and other less-intrusive security screening activities were under-used or not used at all.

12. NSIRA found that the polygraph was de facto determinative in security screening decisions at CSE.

13. NSIRA found that CSE's security screening decision-making may not comply with record-keeping requirements of the Standard on Security Screening.

14. NSIRA found that CSE's use of the polygraph in security screening decisions makes more uncertain the opportunity to challenge denials of security clearances pursuant to the NSIRA Act and the Standard.

15. NSIRA found that TBS did not adequately consider privacy or Charter implications when it included the polygraph as a security screening activity under the Standard on Security Screening.

16. NSIRA found that the Standard on Security Screening insufficiently addresses Charter and privacy implications related to the use of the polygraph.

17. NSIRA found that the Government of Canada's current use of the polygraph for security screening in the manner described in this review may raise serious concerns in relation to the *Canadian Charter of Rights and Freedoms*.

NSIRA's recommendations

Recommendation 1: NSIRA recommends that the Treasury Board of Canada urgently remedy the issues identified by this review related to the legality, reasonableness and necessity of the use of the polygraph for security screening in Canada, or remove it from the Standard on Security Screening.

NSIRA's recommendations

Recommendation 2: NSIRA recommends that CSE urgently remedy the issues identified by this review, including Charter and *Privacy Act* compliance, or cease conducting polygraph exams for security screening.

Review of CSE's Network-based solutions and related Cybersecurity & Information Assurance activities

NSIRA's findings

1. NSIRA found that CSE operates a comprehensive and integrated ecosystem of cybersecurity systems, tools, and capabilities to protect against cyber threats, with a design that incorporates measures meant to protect the privacy of Canadians and persons in Canada.

2. NSIRA found that CSE treated all network-based solutions (NBS) information as information related to a Canadian or a person in Canada (IRTC), and applied measures intended to protect privacy to all NBS-acquired information.

3. NSIRA found that information acquired through NBS will, by its nature, always include information related to a Canadian or person in Canada (IRTC) and is certain to include some information for which there is a reasonable expectation of privacy (REP) of a Canadian or person in Canada. This was not transparently communicated in corresponding applications to the Minister.

4. NSIRA found that, due to a lack of clarity in its relationship with SSC, CSE did not obtain consent from system owners for its cybersecurity and information assurance activities in the way described to the Minister.

5. NSIRA found that SSC was not fully aware of its responsibilities as a system owner, as described in CSE's applications to the Minister.

6. NSIRA found that, despite the existence of a Memorandum of Understanding between CSE and SSC, there was a lack of clarity between the organizations on the implementation of agreed-upon commitments about NBS activities on networks operated by SSC.

7. NSIRA found that CSE did not explain to the Minister why consent to CSE's cybersecurity activities could not reasonably be obtained from users of Government of Canada systems.

8. NSIRA found that CSE's narrow application of subsection 22(4) of the CSE Act introduces legal and accountability risks and resulted in CSE acquiring information that may interfere with a reasonable expectation of privacy of a Canadian or person in Canada. This information was from a source acquired outside of the scheme of Ministerial authorizations.

9. NSIRA found that an incongruence between subsections 27(1) and 22(4) of the CSE Act prevents CSE from acquiring certain information from [*specific type of*] sources such as [*specific information source*], where this information interferes with the reasonable expectation of privacy of a Canadian or person in Canada. Some of this information would enhance CSE's ability to fulfill its cybersecurity and information assurance mandate.

NSIRA's recommendations
Recommendation 1: NSIRA recommends that CSE clearly explain, in its applications to the Minister, that: • Network-based solutions acquire information relating to a Canadian or a person in Canada (IRTC), including information that interferes with the reasonable expectation of privacy (REP) of Canadians or persons in Canada; and, • CSE subsequently uses, analyses, and retains this information for use in cybersecurity and information assurance activities.
Recommendation 2: NSIRA recommends that CSE renew its Memorandum of Understanding with SSC to ensure CSE and SSC meet their respective commitments, including any that CSE makes to the Minister regarding SSC's role in informing system owners about the NBS program.
Recommendation 3: NSIRA recommends that CSE update Memoranda of Understanding with all of its cybersecurity partners, to ensure these partners have consented to CSE cybersecurity activities, and to ensure these arrangements reflect, and conform to, contemporary governance authorities. CSE should continue these updates, as a standard practice, as authorities evolve.
Recommendation 4: NSIRA recommends that CSE explain to the Minister how consent to CSE's cybersecurity activities is obtained from users of Government of Canada systems, or otherwise explain why this consent could not reasonably be obtained.
Recommendation 5: NSIRA recommends that CSE reconsider whether limits on the acquisition by CSE of information from the global internet infrastructure (as per subsection 22(4) of the CSE Act) apply to information [*specific source of information*] sources. This should include an assessment of whether section 8 of the *Charter of Rights and Freedoms* may be engaged, as well as cases where [*specific source of information*] sources may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada.
Recommendation 6: NSIRA recommends that, in order to continue these acquisition activities that are necessary for cybersecurity and information assurance (CSIA) purposes, CSE assess its current sources

NSIRA's recommendations
of CSIA information—that are acquired outside of an Authorization—for interference with the reasonable expectation of privacy of a Canadian or person in Canada. This assessment should be repeated as required to ensure such information is not acquired without a valid Ministerial authorization.
Recommendation 7: NSIRA recommends that section 27 of the CSE Act be amended to permit the Minister to authorize CSE to acquire information that is necessary for CSE's cybersecurity and information assurance aspect (but which may contain information that interferes with the reasonable expectation of privacy of a Canadian or person in Canada, or contravene an Act of Parliament), from sources other than federal information infrastructures and systems of importance to the Government of Canada.

Canada Border Services Agency review

Review of the CBSA's Confidential Human Source Program

NSIRA's findings

1. NSIRA found that CBSA policy does not require any documented approval or a documented assessment of the risks of using a CHS outside of the registration process.

2. NSIRA found that there was incomplete documentation in the preregistration period such that the CHS Program is impeded from monitoring the full spectrum of CHS Program activities.

3. NSIRA found that CBSA's policies and practices around obtaining informed consent are insufficient to ensure that it is obtained systematically, and before individuals incur the risks of providing information in confidence to CBSA.

4. NSIRA found that measures to mitigate risks to CHSs are often not present or implemented.

5. NSIRA found that CBSA may have breached the law of informer privilege in two instances.

6. NSIRA found that Inland Enforcement Officers collected information and promised confidentiality, but did so without training under the applicable policy to support a proper understanding of the consequences of extending confidentiality.

7. NSIRA found that CBSA's approach to risk management in their new policy suite does not fully align with principles in the MD.

8. NSIRA found that the information CBSA will provide to the Minister as required by Ministerial Direction is not sufficient to convey the size and scope of the Confidential Human Source Program.

9. NSIRA found that in two cases the CBSA did not comply with subsection 12(2) of the CBSA Act in that it failed to follow the MD's requirement to inform the Minister when there was a Confidential Human Source activity that "may have significant adverse impact such as impacting the safety of an individual".

NSIRA's recommendations
Recommendation 1: NSIRA recommends that CBSA amends its policy to require a documented risk assessment and formal approval for using a CHS in the preregistration period.
Recommendation 2: NSIRA recommends that CBSA require that the interview checklist be administered no later than when the promise of confidentiality is extended.
Recommendation 3: NSIRA recommends that CBSA provide guidance as to how obtaining informed consent should be tailored to the individual circumstances of the CHS.
Recommendation 4: NSIRA recommends that CBSA put in place specific guidance on how to mitigate the full range of risks to CHSs and ensure that those mitigation measures are implemented.
Recommendation 5: NSIRA recommends CBSA expand its definition of active Confidential Human Source so that reporting to the Minister covers the breath of the CHS program.
Recommendation 6: NSIRA recommends that CBSA immediately notify the Minister of the two cases identified in this review where safety of an individual is at issue.

Department of National Defence and the Canadian Armed Forces Review

Review of DND/CAF's Human Source Handling Program

NSIRA's findings

1. NSIRA found that DND/CAF's policy framework allows human source handling activities that may not be in compliance with the law.

2. NSIRA found that DND/CAF policy is insufficiently specific with respect to recognizing and avoiding mistreatment risks created by human source handling activities.

3. NSIRA found that DND/CAF's risk assessment framework for human source handling operations is inadequate. The current assessments of risk do not provide adequate or reliable information to decision-makers because they:

    - are overly subjective;
    - do not present mitigated and unmitigated risks clearly;
    - conflate risks; and
    - narrowly focus the considerations of certain risks at the expense of others.

4. NSIRA found gaps in the discharge of DND/CAF's duty of care from engagement of the human source to disengagement. These gaps include:

    - a safeguard process that is not appropriately engaged for certain sources;
    - an underdeveloped complaints process for sources; and
    - insufficient assessments of the risk posed to Agents.

5. NSIRA found that the Minister of National Defence is not adequately informed in order to fulfill ministerial accountabilities for human source handling operations.

6. NSIRA found that further ministerial direction is required to support the governance of DND/CAF's human source handling program.

NSIRA's recommendations
Recommendation 1: NSIRA recommends that Parliament enact a justification framework to authorize DND/CAF and its sources to commit acts or omissions outside Canada that would otherwise be unlawful, where reasonable for the collection of defence intelligence.
Recommendation 2: NSIRA recommends that DND/CAF develop policy governance to properly equip Field HUMINT teams to conduct their human source handling activities in compliance with the law. At minimum, this should include: • Increased attention to determine whether individuals are involved in terrorist activity; • governance controls to increase accountability and enable responsiveness; • a change in policy to only accept information with plausible lawful provenance; • the development of training to support CAF members on how to handle human sources while mitigating legal risk; and • a review of operations with respect to their compliance with Canada's foreign legal obligations.
Recommendation 3: NSIRA recommends that DND/CAF adopt an approach for assessing whether its exchanges with human sources create a substantial risk of mistreatment that is specific to human

NSIRA's recommendations
source handling, comprehensive with respect to its obligations in international human rights law and international humanitarian law, and formalized in policy and procedure.
Recommendation 4: NSIRA recommends that DND/CAF develop a risk assessment framework specific to human source handling, with appropriate doctrinal guidance for the assessment of human sources that includes consideration of all relevant risk factors. All DND/CAF members implicated in the risk assessment process (including field HUMINT team members, commanders, intelligence staff, and legal and policy advisors) should be appropriately trained on the new risk assessment framework and guidance to ensure consistency across teams and deployments.
Recommendation 5: NSIRA recommends that DND/CAF adopt, in consultation with other departments as necessary, additional measures aimed at ensuring the welfare and protection of their human sources. These measures should be clearly operationalized in governance documents (directives, orders, procedures, etc.) and should address, at minimum, the issues identified in Finding #3.
Recommendation 6: NSIRA recommends that DND/CAF, in consultation with the Minister of National Defence, improve the content of biannual reports to the Minister to include, at minimum, the legal, policy and governance issues that may impact human source handling operations.
Recommendation 7: NSIRA recommends that, with respect to human source handling operations, DND/CAF create official written records of notifications and briefings to the Minister of National Defence, as well as records of decision to improve mutual accountability.
Recommendation 8: NSIRA recommends that the Minister of National Defence issue ministerial direction on human source handling to DND/CAF that includes, at minimum: • fundamental principles guiding the lawful and ethical conduct of source handling operations; • the types of risk that should be assessed and when these risks should be consulted at the ministerial level; • expectations regarding the management of human sources; and • direction regarding the content and frequency of reporting.

Multi-departmental reviews

Review of Operational Collaboration between CSE and CSIS

NSIRA's findings

1. NSIRA found that CSE does not routinely share its operational plans and associated risk assessments with CSIS when operating under CSIS authorities. This may leave CSIS unable to fully assess CSE's activities for compliance.

2. NSIRA found that close collaboration at the working level created the right conditions for CSIS to monitor CSE's assistance activities for compliance with warrant conditions.

3. NSIRA found that CSIS failed to submit an updated request for assistance to CSE in a timely manner when it sought new warrant powers.

4. NSIRA found that CSE and CSIS did not engage in any joint investigation, assessment, or tracking of a compliance incident.

5. NSIRA found that CSE and CSIS failed to implement an effective operational framework for their collection activity. This contributed to two instances of non-compliance with the Federal Court's direction.

6. NSIRA found that CSE and CSIS identified an effective opportunity to collaborate under their respective mandates and carried out an operation that proved beneficial for both Canada and its allies.

7. NSIRA found that, while CSIS's operational framework was sufficient, CSE's operational framework did not assess legal and policy risk specific to the operation.

8. NSIRA found that CSE and CSIS did not draft joint terms of engagement, a joint operational plan, or engage in joint risk assessments.

9. NSIRA found that CSE's foreignness assessment did not account for the increased risk of targeting Canadians when working with CSIS.

10. NSIRA found that both CSE and CSIS lack policies, procedures, and accountability mechanisms to govern CSIS lead information messages and associated requests and actions.

11. NSIRA found that CSIS's use of lead information messages to share information and make requests about Canadians creates a high risk of potential for non-compliance for CSE.

12. NSIRA found that CSE's application of incidental collection provisions may not be appropriate in situations where CSE knows there is a Canadian nexus to a CSIS foreign intelligence lead, and where it knows it is likely to collect Canadian information in pursuing the lead.

13. NSIRA found that CSE did not comply with section 22(1) of the CSE Act when it [*reviewed the contents*] of a Canadian's device obtained through a CSIS lead information message.

14. NSIRA found that CSE did not comply with either section 22(1) of the CSE Act or section 273.64(2)(a) of the *National Defence Act* (NDA) when it used [*a number of*] complete exceptional reports for foreign intelligence purposes.

15. NSIRA found that CSE does not consistently utilize its protected entity tool to prevent targeting Canadian identifiers it receives from CSIS.

16. NSIRA found that while CSIS performs an initial consultation, it does not routinely pursue further engagement with CSE during Threat Reduction Measure activities that could overlap with CSE activities.

17. NSIRA found that CSE did not notify CSIS in a timely manner of a compliance incident in its Active Cyber Operation, which was connected to a CSIS Threat Reduction Measure.

18. NSIRA found that CSE failed to cooperate effectively with CSIS, leading to a missed opportunity to advance Canadian intelligence objectives via domestic collaboration.

NSIRA's recommendations
Recommendation 1: NSIRA recommends that CSE share its operational plans and associated risk assessments with CSIS prior to operating under CSIS authorities.
Recommendation 2: NSIRA recommends that when CSIS engages CSE for assistance with the execution of warranted powers, a CSIS employee be involved to ensure compliance in CSE's collection activities until the request for assistance has terminated.
Recommendation 3: NSIRA recommends that CSIS develop a process to ensure that necessary requests for assistance are submitted to CSE in a timely manner subsequent to obtaining warrant powers.

NSIRA's recommendations
Recommendation 4: NSIRA recommends when working under a request for assistance CSIS and CSE develop a framework for joint investigation of potential compliance incidents.
Recommendation 5: NSIRA recommends that CSIS ensure roles and responsibilities are clearly agreed to prior to allowing partners to execute warrant powers. Where appropriate, these agreements should be shared with the Federal Court.
Recommendation 6: NSIRA recommends that CSIS ensure it is directly involved in all substantive communications with any partner actively executing its warrant powers.
Recommendation 7: NSIRA recommends that CSIS share paragraphs 32 through 41 of this review, along with associated recommendations, with the Federal Court.
Recommendation 8: NSIRA recommends that when CSE engages in joint operations with CSIS it should perform risk assessments for each operational activity. These should specifically consider the risk of targeting Canadians and implement proactive measures to mitigate this risk.
Recommendation 9: NSIRA recommends that when participating in joint operations, CSE and CSIS either jointly develop or share written terms of engagement, operational plans, and risk assessments.
Recommendation 10: NSIRA recommends that CSE perform foreignness assessments that account for the increased risk of targeting Canadians when working with CSIS.
Recommendation 11: NSIRA recommends CSIS cease making requests for action and/or further information to CSE in relation to Canadians or people in Canada via CSIS lead information messages.
Recommendation 12: NSIRA recommends that CSIS develop policies, procedures, and analyst training to standardize the disclosure of CSIS lead information messages to CSE.
Recommendation 13: NSIRA recommends that CSE develop policies, procedures, and analyst training to standardize the use of CSIS lead information messages.
Recommendation 14: NSIRA recommends that CSE develop a regime for collecting, retaining, and reporting to CSIS Canadian information it uncovers further to legitimate foreign intelligence activities where it has advance knowledge of the Canadian information.
Recommendation 15: NSIRA recommends that CSE update its policies to prohibit the analysis of information relating to a Canadian or person in Canada for the purposes of identifying foreign intelligence.

NSIRA's recommendations
Recommendation 16: NSIRA recommends that if CSIS decides to disclose exceptional reporting to CSE, it should extract the relevant foreign intelligence for disclosure as opposed to sending the entire report.
Recommendation 17: NSIRA recommends that CSE cease using complete exceptional reports from CSIS under its foreign intelligence mandate.
Recommendation 18: NSIRA recommends that CSE introduce a requirement to always apply the protected entity tool to all Canadian identifiers.
Recommendation 19: NSIRA recommends that CSIS pursue routine engagement with CSE during the implementation of its Threat Reduction Measures when the potential for operational overlap exists.
Recommendation 20: NSIRA recommends that CSE share details of potential compliance incidents with CSIS when an overlap may exist with a CSIS Threat Reduction Measure.

Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2022[17]

NSIRA's findings

1. NSIRA found that CSE, CSIS, GAC, and IRCC regularly use the SCIDA in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of the SCIDA.

2. NSIRA found that CBSA, DND/CAF, and IRCC were non-compliant with subsection 9(3) of the SCIDA, as they failed to provide all records created under subsections 9(1) or 9(2) to NSIRA within the legislated timeframe.

3. NSIRA found improved compliance outcomes in instances where departments prepared record overview spreadsheets under subsections 9(1) and 9(2) of the SCIDA that displayed the following characteristics:

    - a row for each disclosure made or received;
    - columns explicitly tied to each individual paragraph under section 9; and

[17] See full redacted review: https://nsira-ossnr.gc.ca/en/publications/secretariat-operations/review-of-government-of-canada-institutions-disclosures-of-information-under-the-security-of-canada-information-disclosure-act-in-2022/

- additional columns to capture relevant administrative details, such as whether the disclosure was requested or proactive; the date of the request (if applicable); and any applicable file reference numbers.

4. NSIRA found that all GC institutions complied with their obligation to prepare and keep records that set out the information prescribed under subsections 9(1) and 9(2) of the SCIDA.

5. NSIRA found that more than half of the descriptions provided by CBSA and IRCC under paragraph 9(1)(e) of the SCIDA did not explicitly address their satisfaction that the disclosure was authorized under paragraph 5(1)(b), the proportionality test.

6. NSIRA found, within the sample of disclosures reviewed, that disclosing institutions demonstrated they had satisfied themselves of both the contribution and proportionality tests, in compliance with subsection 5(1) of the SCIDA.

7. NSIRA found that GAC satisfied itself under the SCIDA's paragraph 5(1)(a) contribution test based on an incorrect understanding of the recipient's national security mandate in two cases.

8. NSIRA found, within the sample of disclosures reviewed, that CBSA and GAC (in one and two disclosures, respectively) were non-compliant with the SCIDA's subsection 5(2) requirement to provide a statement regarding accuracy and reliability.

9. NSIRA found, in relation to the remaining disclosures within the sample, that GAC, IRCC, and RCMP included their statements regarding accuracy and reliability within the disclosures themselves, whereas CBSA provided its statements in the disclosures' cover letters.

10. NSIRA found that DND/CAF destroyed information under the SCIDA subsection 5.1(1), but they were non-compliant with the requirement to do so "as soon as feasible after receiving it."

11. NSIRA found delays between when a disclosure was authorized for sending and when it was received by the individual designated by the head of the recipient institution to receive it in at least 20% (n=34) of disclosures.

NSIRA's recommendations

Recommendation 1: NSIRA recommends that information sharing arrangements be used to govern regular SCIDA disclosures between GAC and CSIS; IRCC and CSIS; as well as IRCC and CSE.

NSIRA's recommendations
Recommendation 2: NSIRA recommends that all GC institutions prepare record overviews to clearly address the requirements of subsections 9(1) and 9(2) of the SCIDA; and provide them to NSIRA along with a copy of the disclosure itself and, where relevant, a copy of the request.
Recommendation 3: NSIRA recommends that disclosing institutions explicitly address the requirements of both paragraphs 5(1)(a) and 5(1)(b) in the records that they prepare under paragraph 9(1)(e) of the SCIDA.
Recommendation 4: NSIRA recommends that GC institutions contemplating the use of proactive disclosures under the SCIDA communicate with the recipient institution, ahead of making the disclosure, to inform their assessments under subsection 5(1).
Recommendation 5: NSIRA recommends that all disclosing institutions include statements regarding accuracy and reliability within the same document as the disclosed information.
Recommendation 6: NSIRA recommends that GC institutions review their administrative processes for sending and receiving disclosures under the SCIDA, and correct practices that cause delays.

Review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2022

NSIRA's findings

1. NSIRA found that all departments, with the exception of DFO in respect of subsection 7(1), complied with the reporting requirements set out in the ACA.

2. NSIRA found that all departments had frameworks to govern their implementation of the ACA and its associated directions by the end of 2022.

3. NSIRA found that most departments demonstrated continual refinements of their ACA frameworks based on self-identified gaps, NSIRA recommendations, and community-wide coordination efforts.

4. NSIRA found that TC's ACA governance framework did not include policies and procedures for:

    a) escalating cases to the deputy head; or

    b) assessing the risks of information sharing with foreign entities.

5. NSIRA found that all departments, with the exception of DFO, GAC, PS, and TC, used country and/or entity risk assessments to inform their assessments of substantial risk of mistreatment and corresponding case escalation.

6. NSIRA found that departments' country risk assessments were inconsistent with one another.

7. NSIRA found that the simultaneous conduct of independent human rights risk assessments in different departments reflected a substantial duplication of effort across the GC, and created the opportunity for discrepant outcomes.

8. NSIRA found, for the fourth consecutive year, that no departments escalated cases to their deputy heads for determination or decision.

9. NSIRA found that some high-risk sharing activities were stopped prior to escalation for consideration of possible mitigations.

10. NSIRA found that certain departments' ACA governance frameworks and risk assessment methodologies included features that may systematically under-assess the level of risk involved in a transaction. These features include:

    - discrepant applications of the threshold for substantial risk of mistreatment;
    - incorporating mitigations into baseline assessments of risk, while overestimating their effects; and
    - a lack of checks and balances in the risk assessment process.

NSIRA's recommendations

Recommendation 1: NSIRA recommends that TC update its ACA governance framework to include policies and procedures for:

a) escalating cases to the deputy head; and

b) assessing the risks of information sharing with foreign entities.

Recommendation 2: NSIRA recommends that the Government of Canada designate a body responsible for developing:

a) a unified set of assessments of the human rights situations in foreign countries including a standard "risk of mistreatment" classification level for each country; and

b) to the extent that multiple departments deal with the same foreign entities in a given country, standardized assessments of the risk of mistreatment of sharing information with foreign entities.

NSIRA's recommendations
Recommendation 3: NSIRA recommends that departments apply the "substantial risk" threshold in a manner consistent with the definition adopted government-wide; and that departments whose broader policy frameworks do not yet reflect this definition (CBSA, CRA, IRCC, and TC) make the attendant updates.
Recommendation 4: NSIRA recommends that departmental assessments of substantial risk of mistreatment be grounded in countries' human rights records; and that subsequent entity-level considerations be based on validated, current, and consistent respect for caveats and assurances, rather than the absence of derogatory information particular to that entity or other bilateral considerations.
Recommendation 5: NSIRA recommends that all ACA governance frameworks incorporate layered checks and balances in the risk assessment and escalation of cases that may involve substantial risk of mistreatment.

Annex C: Statistics on complaints investigations

January 1–December 31, 2023

INTAKE INQUIRIES		135
New complaints filed		**26**
National Security and Intelligence Review Agency Act (NSIRA Act), section 16, Canadian Security and Intelligence Service (CSIS) complaints		18
NSIRA Act, section 17, Communications Security Establishment (CSE) complaints		5
NSIRA Act, section 18, security clearances		3
NSIRA Act, section 19, Royal Canadian Mounted Police (RCMP) referred complaints		0
NSIRA Act, section 19, *Citizenship Act*		0
NSIRA Act, section 45, Canadian Human Rights Commission (CHRC) referrals		0
Accepted jurisdiction to investigate		**8**
	Accepted	Declined
NSIRA Act, section 16, CSIS complaints	6	17
NSIRA Act, section 17, CSE complaints	1	4
NSIRA Act, section 18, security clearances	0	1
NSIRA Act, section 19, RCMP referred complaints	1	0
Total	8	22
Active investigations as of December 31, 2023		**17**
NSIRA Act, section 16, CSIS complaints		8
NSIRA Act, section 17, CSE complaints		1
NSIRA Act, section 18, security clearances		4
NSIRA Act, section 19, RCMP referred complaints		3

NSIRA Act, section 19, continuation of investigation (RCMP referred complaint) [a]				1
Informal resolution in progress as of December 31, 2023				**1**
NSIRA Act, section 16 (CSIS complaints)				0
NSIRA Act, section 17 (CSE complaints)				0
NSIRA Act, section 18 (security clearances)				1
NSIRA Act, section 19 (RCMP referred complaints)				0
Total investigations closed				**12**
	Abandoned	**Final report**	**Resolved informally**	**Withdrawn**
NSIRA Act, section 16, CSIS complaints	0	4	3	0
NSIRA Act, section 17, CSE complaints	0	0	1	0
NSIRA Act, section 18, security clearances	0	0	0	0
NSIRA Act, section 19, RCMP referred complaints	1	3	0	0
NSIRA Act, section 45, CHRC referrals	0	0	0	0
Total	1	7	4	0

[a] First final report was issued in 2022. The continuation is a remaining issue.