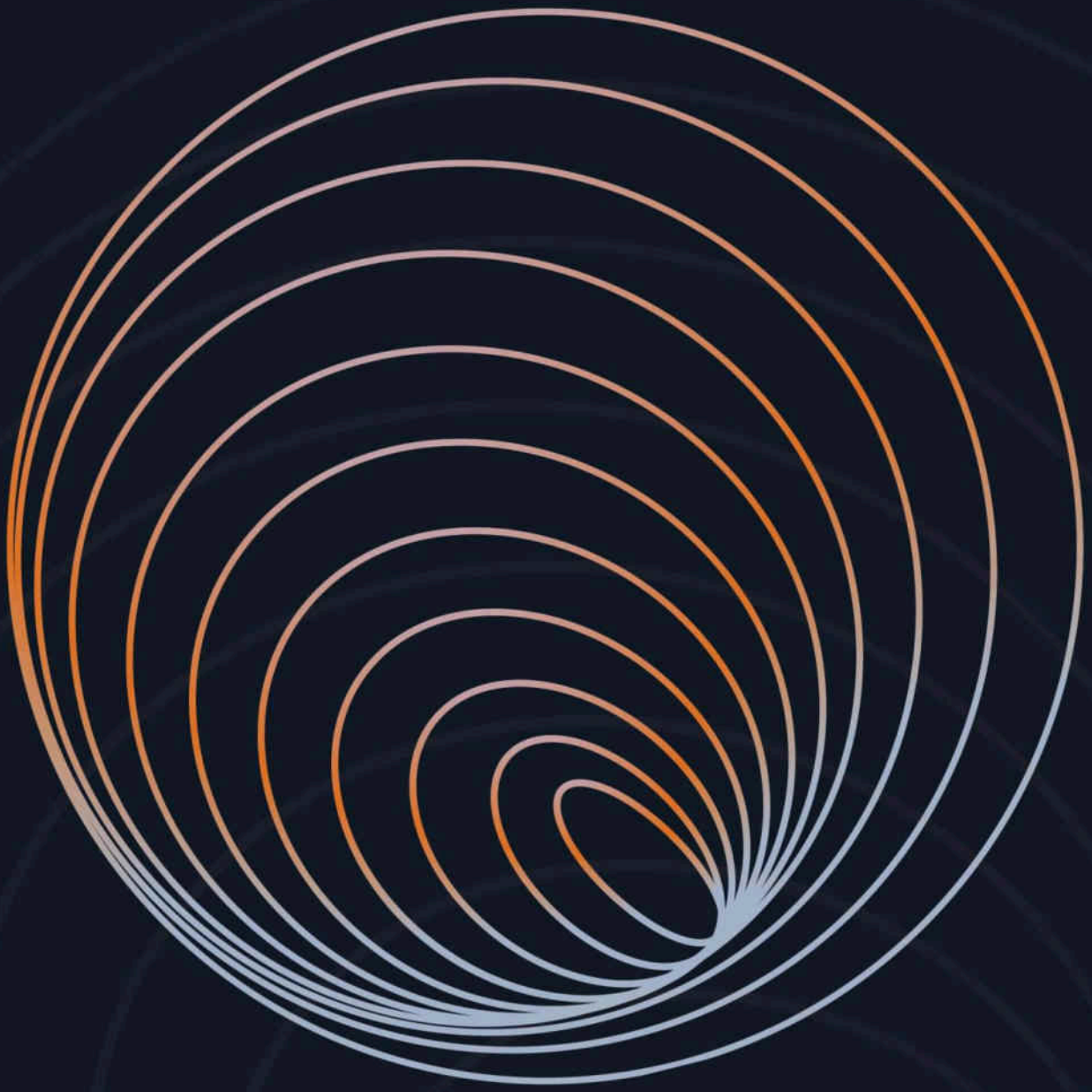
National Security and Intelligence Review Agency | Office de surveillance des activités en matière de sécurité nationale et de renseignement

Canada

National Security and Intelligence Review Agency

2024 // Annual Report



© His Majesty the King in Right of Canada, as represented
by the National Security and Intelligence Review Agency, 2025.
ISSN: 2563-5778
Catalogue No. PS106-9E-PDF

Table of Contents

Message from the members ..... **v**

Executive Summary ..... **vi**

Reviews vi

Complaint Investigations vi

01 // NSIRA in Context **1**

1.1 About NSIRA 1

1.2 NSIRA's Vision and Mission 2

1.3 Unique Functions of NSIRA 2

1.4 NSIRA's Domestic Partnerships 3

1.5 Sustaining an Independent Review Body 3

1.6 Protecting Democracy and Freedoms 4

1.7 Transparency and Engagement 4

1.8 NSIRA's Role on the World Stage 5

02 // Highlights on Key Initiatives **7**

2.1 Reviewee Responsiveness 7

2.2 Follow-Up on Recommendations 7

2.3 Investigations: Volume Increase and Streamlining Processes 8

2.4 Three-Year Strategic Plan 8

2.5 New Offices Built to High Standards 9

03 // Reviews **10**

3.1 Overview 10

3.2 CSIS Reviews 11

3.3 CSE Reviews 17

3.4 Other Department Reviews 17

3.5 Multi-Departmental Reviews 22

04 // Complaint Investigations **40**

4.1 Overview 40

4.2 Ongoing Initiatives 41
4.3 Investigation Report Summaries 41
4.4 Other Outcomes 46
4.5 Statistics on Complaint Investigations 47
05 // Looking Ahead 51
5.1 Advancing NSIRA's Vision 51
06 // Annexes 52
Annex A: Abbreviations 52
Annex B: Statistics and Data 54

Message from the members

The National Security and Intelligence Review Agency (NSIRA, Review Agency) is pleased to present its 2024 Annual Report, highlighting key achievements, progress, and our direction for coming years.

2024 Key Highlights

In 2024, NSIRA observed a **notable increase in the number of complaint investigations linked to immigration security screening delays**.

Additionally, NSIRA has released its **first Section 40 public interest report** this year, marking an important milestone in its mandate. This report underscores NSIRA's dedication to transparency and accountability in national security matters.

NSIRA's 2024–2027 Strategic Plan

After five years of operation, NSIRA has developed its triennial strategic plan for 2024-2027, which will guide the Review Agency's efforts in the coming years. The strategic plan focuses on NSIRA's commitment to enhancing review; investigating complaints in a timely, fair, and efficient manner; fostering transparency; and strengthening public trust in NSIRA's rigorous, fully independent review approach to Canada's national security and intelligence activities.

NSIRA's Role on the International Stage

NSIRA continues to strengthen its international partnerships, ensuring its work remains informed by, and a contributor to, global best practices in review. By engaging with international counterparts, NSIRA positions Canada as an active leader in upholding democratic values on the global stage.

We would like to thank the staff of NSIRA's Secretariat for their expertise, efforts and resilience throughout this ambitious year and for their innovation, energy and commitment for the year ahead.

Marie Deschamps	**Craig Forcese**	**Foluke Laosebikan**
Colleen Swords	**Matthew Cassar**	**Jim Chu**

Executive Summary

1. Without specialized national security review, much security service conduct would be immunized from scrutiny by reason of national security secrecy. The National Security and Intelligence Review Agency (NSIRA)'s raison d'être is to ensure that there is no such immunity. NSIRA has two mandates: conducting national security reviews of security or intelligence activities and conducting investigations of complaints from the public brought against a subset of national security and intelligence services.
2. In five years of existence, NSIRA has become a robust and professional review body that conducts reviews and investigates public complaints, which reflect the highest standards and core values of Canadian society: democracy, transparency and the rule of law.
3. This 2024 Annual Report outlines the multiple spheres of activity through which NSIRA has contributed meaningfully to shaping the landscape of national security and intelligence review. This work is central to strengthening public trust, ensuring democratic oversight, and safeguarding the rights and freedoms of all Canadians.

Reviews

4. The Reviews section of this report provides a summary of each of the nine review reports that were approved by Members during 2024, including the *Review of the Dissemination of Intelligence on People's Republic of China Political Foreign Interference*, which resulted in NSIRA's first special report tabled under section 40 of the NSIRA Act, where NSIRA determined that releasing the report and its conclusions to Parliament was in the public interest. The review reports that NSIRA presented to the relevant departments and agencies in 2024 contain 67 findings and 45 recommendations.

Complaint Investigations

5. During the last five months of 2024, NSIRA observed a significant increase of public complaints against CSIS, alleging process delays in immigration or citizenship security screening which resulted in NSIRA ingesting an unprecedented number of new complaints.

01 //

NSIRA in Context

1.1 About NSIRA

6. The National Security and Intelligence Review Agency (NSIRA, the Review Agency) is an independent entity that reviews and investigates public complaints related to national security or intelligence activities to assess their lawfulness, reasonableness, and necessity. NSIRA may have up to seven Members, supported by a Secretariat with expertise in law, technology and national security, and led by an Executive Director appointed by the Governor-in-Council.
7. NSIRA has two mandates: reviewing Government of Canada national security or intelligence activities and investigating public complaints related to those activities.
8. NSIRA's approach in managing its review process is innovative. Review teams are comprised of individuals with diverse skill sets. They execute reviews under the direction of a designated NSIRA member and relevant Secretariat management personnel. Similarly, NSIRA's model for investigations of complaints relies on an NSIRA Member serving in a quasi-judicial investigative role, supported by legal, registry, and research staff.

1.2 NSIRA's Vision and Mission



1.3 Unique Functions of NSIRA

9. NSIRA holds a unique and pivotal position within Canada's national security accountability framework. With a mandate spanning the entire federal government, NSIRA can review any national security or intelligence activity, irrespective of the department or agency involved. This extensive jurisdiction enables NSIRA to carry out comprehensive, integrated, in-depth reviews of sensitive operations.
10. NSIRA also functions as a complaint investigation body, primarily examining national security-related allegations against the Canadian Security Intelligence Service (CSIS) or the Communications Security Establishment (CSE), activities of the Royal Canadian Mounted Police (RCMP) closely related to national security, and denials of security clearance by federal departments. These public complaints often involve serious allegations, and NSIRA's capacity to address them enhances access to justice and the protection of individual rights.
11. With access to classified and legally privileged information, NSIRA is uniquely equipped to examine whether national security powers are exercised in compliance with Canadian law.

1.4 NSIRA's Domestic Partnerships

12. As part of Canada's national security and intelligence accountability framework, NSIRA and the National Security and Intelligence Committee of Parliamentarians (NSICOP) serve complementary yet distinct roles. While both play crucial roles in ensuring accountability, they differ in structure and mandate.
13. NSICOP is a committee of parliamentarians and focuses its reviews on the effectiveness of the national security and intelligence agencies. It is impacted by events such as elections or dissolutions. NSICOP's makeup makes it uniquely well positioned to examine both the efficacy of the national security and intelligence community, in particular, its legal frameworks, and broad strategic trends across the national security landscape.
14. NSIRA operates year-round and maintains consistent engagement regardless of the Parliamentary schedule. Its mandate is to focus on the legality and legal compliance of national security and intelligence activities through in-depth reviews that dig down vertically into the operational events conducted on the ground. To deliver on its mandate to investigate complaints, NSIRA's continuous operations are essential to ensuring that investigations are conducted without delay.
15. NSIRA and NSICOP both enhance transparency and accountability in national security via their distinct mandates, which ensures a complete approach to independent review. They actively coordinate efforts and avoid duplication. The respective secretariats have established a strong working relationship. Together, NSICOP and NSIRA form a complementary system supporting democratic accountability and continuous legal scrutiny.
16. NSIRA is committed to working within a system of partnerships with key actors. It is part of a larger network of federal review and accountability bodies and regularly engages with the Civilian Review and Complaints Commission, the Office of the Intelligence Commissioner, the Office of the Auditor General, and the Office of the Privacy Commissioner (OPC). These collaborations are about best practices, ensuring aligned mandates, minimizing redundancy, and reinforcing a broader framework of transparency.

1.5 Sustaining an Independent Review Body

17. NSIRA's independence is the cornerstone of its credibility and effectiveness as a national security review body. Operating independently from the executive branch,

NSIRA conducts impartial and expert reviews of Canada's most sensitive security and intelligence activities. This institutional autonomy is not just a privilege, it is an attitudinal necessity and a responsibility that NSIRA takes seriously. It's vital for preserving the integrity of its operations and cultivating public trust.

18. The NSIRA Act grants access to all information held by reviewed departments, including classified and legally protected information, except for Cabinet confidences. This access allows NSIRA to independently review the legality, necessity, and proportionality of government actions.

19. NSIRA's reports, findings, and recommendations are not subject to any editorial control from the prime minister or any other minister, nor are they subject to any editorial control from senior officials. This approach preserves NSIRA's voice and commitment to transparency and accountability.

20. To uphold this independence, NSIRA invests in secure digital systems, enhances internal governance, and develops expertise through targeted hiring and training. These initiatives improve the professionalism and integrity of NSIRA's work.

1.6 Protecting Democracy and Freedoms

21. NSIRA ensures Canada's national security activities align with the rule of law and the *Canadian Charter of Rights and Freedoms*, enhancing public confidence in Canada's national security framework. NSIRA's role is vital in upholding a national security system based on legality and democratic accountability.

22. In 2024, NSIRA's reviews tackled foreign interference, bulk data, and technology-enabled intelligence activities. NSIRA's findings led to recommendations to keep these powers within legal and ethical limits. By reviewing the extraordinary powers of the national security community, NSIRA plays a vital role in preserving the integrity of the rule of law in Canada.

1.7 Transparency and Engagement

23. Transparency is a core value at NSIRA, shaping how the Review Agency conducts its work. Increasing public understanding of NSIRA's work and its findings and recommendations is a fundamental value of the organization. NSIRA aims to ensure that Parliamentarians, media, civil society, academia, and the broader Canadian public remain engaged in its work, enabling them to form their

independent views on national security or intelligence issues and to hold government accountable.

24. In the challenging context of national security operations, absolute public transparency could unfortunately provide adversaries and threat actors with information that might harm Canada's security interests, as well as those of its allies. NSIRA applies a rigorous balanced approach to release as much information as possible about its work in its commitment to transparency and openness, while safeguarding genuinely injurious national security information.

25. In 2024, NSIRA enhanced its public reporting efforts by announcing on social media each time a report was submitted to a Minister and by informing the public that reports can be accessed under the *Access to Information Act*. NSIRA also began publishing backgrounders to provide Canadians with greater clarity on the context of its reviews. As part of its commitment to openness, the Agency launched an updated and more accessible website.

26. Additionally, in 2024, NSIRA expanded its outreach initiatives to enhance public awareness and understanding of its mandate. NSIRA hosted new events with civil society, media, and academia. These initiatives aimed to deepen the understanding of NSIRA's role and to foster informed dialogue about NSIRA's work.

1.8 NSIRA's Role on the World Stage

27. NSIRA's partnerships extend beyond Canada's borders through its active role in the Five Eyes Intelligence Oversight and Review Council (FIORC). As a permanent member, NSIRA actively collaborates with review agencies from Australia, New Zealand, the United Kingdom and the United States, fostering robust collaboration and knowledge exchange.

28. NSIRA has established strong partnerships with European counterparts, including agencies involved in the Intelligence Oversight Working Group made up of Belgium, Denmark, the Netherlands, Norway, Sweden, Switzerland, and the United Kingdom. These partnerships transcend routine collaboration, enabling collective learning on review methodologies and facilitating coordinated knowledge exchange on the development of international review best practices.

29. NSIRA has also been an active collaborator in some initiatives led by certain United Nations divisions that aim to improve global partnerships in the review and oversight sector. This has led to engagement with new international partners,

delivery on online training modules, and new contributions to global standards in review.

30. Through these international engagements, NSIRA plays an active role in shaping a global community of practice that promotes the values of rigorous independent review of national security or intelligence activities.

02 //

Highlights on Key Initiatives

2.1 Reviewee Responsiveness

31. Access to information is fundamental to NSIRA's ability to conduct effective reviews and investigations. In 2024, NSIRA observed encouraging progress in the responsiveness of several reviewees, particularly regarding the timeliness and completeness of their responses.

32. Despite these improvements, frustrations persist: overbroad, unsubstantiated or excessive demands for redactions in access to information consultations are occurring in every file, inconsistent disclosures in response to requests for information are routine, institutional resistance to NSIRA's access rights occurs, and outdated departmental information systems at times impede NSIRA's ability to conduct its work. NSIRA raises these issues with senior departmental officials and escalates to the Minister when necessary, with mixed results. While responsiveness performance varies across departments, it is fair to say that the status quo is one where process challenges regularly challenge NSIRA's ability to deliver on its mandate. NSIRA is looking at ways to provide better real-time public awareness of its responsiveness challenges so that relevant departments can be held accountable.

2.2 Follow-Up on Recommendations

33. Monitoring the execution of recommendations is pivotal to NSIRA's commitment to facilitate systemic improvement. In 2024, NSIRA strengthened its follow-up practices by initiating dedicated review cycles designed to evaluate the implementation of prior recommendations. The timeliness and comprehensiveness of recommendation responses differ among departments and agencies.

34. To facilitate this endeavour, NSIRA is in the process of developing internal tracking tools and protocols to assist in ensuring more consistent awareness, follow-up, and public communications about institutional responses and progress on NSIRA's recommendations. NSIRA will continue to make advances in the years to come on this significant initiative.

2.3 Investigations: Volume Increase and Streamlining Processes

35. In 2024, NSIRA addressed a surge of CSIS-related complaints from the public tied to delays in immigration and citizenship screening. More than half of the new complaints related to such delays. Several of those new complaints resulted in informal resolutions.

36. NSIRA advanced initiatives to improve and streamline its investigative processes and procedures, as detailed in this report's *Complaint Investigations* section.

2.4 Three-Year Strategic Plan

37. In 2024, NSIRA finalized its 2024-2027 Strategic Plan, setting a clear direction for its priorities over the next three years. The plan reaffirms NSIRA's core values — Independence, Professionalism, Transparency, and Inclusiveness — and serves as a foundation for continuous improvement. It positions both NSIRA and its Secretariat to deliver effective, forward-looking review and investigations of public complaints. NSIRA aims to maintain the highest standards by focusing on contemporary issues, applying rigorous methodologies, delivering on its mandates with impartiality and efficiency, and continuing to modernize NSIRA's processes and leverage new technologies to accomplish improved outcomes for Canadians.

38. To support NSIRA's mission, the strategic plan invests in sustainable corporate infrastructure. This includes fostering a culture of continuous learning and maintaining high standards in information management, security, and human resources. The NSIRA Secretariat strives to be an agile and efficient workplace that attracts and retains top talent.

39. NSIRA also emphasizes its continued collaboration with domestic and international partners to strengthen its review and investigative capabilities. NSIRA aspires to be a globally recognized centre of excellence and a hub for a professional community dedicated to national security accountability. Through this

strategic vision, NSIRA reaffirms its role as the trusted eyes and ears of Canadians in an evolving security landscape.

2.5 New Offices Built to High Standards

40. Between 2021 and 2024, NSIRA's Secretariat led the planning, development, and delivery of a new office space for its staff. This complex undertaking involved meeting the highest standards of security, functionality, and design, all while supporting NSIRA's growing operational needs. Despite tight timelines and evolving requirements, the Secretariat successfully transitioned into the new space efficiently, securely, and with minimal disruption to NSIRA's core mandate.

03 //

Reviews

3.1 Overview

41. NSIRA's review mandate is outlined in subsection 8(1) NSIRA Act and includes reviewing national security or intelligence activities of CSE and CSIS, as well as those of any other federal departments and agencies.
42. The review reports presented in 2024 to the relevant departments and agencies contain 67 findings, and NSIRA issued 45 recommendations.
43. **Table 1** lists the reviews that gave rise to the reports produced and submitted to the responsible minister(s) by NSIRA, in 2024.

Table 1. NSIRA review activities during 2024

Review	Department(s)	Status**
22-07—Canadian Security Intelligence Service Lifecycle of Warranted Information	CSIS	Published
23-05—Annual Review of Select CSIS activities	CSIS	Submitted
23-02—Annual Review of Select CSE Activities	CSE	Submitted
23-10—Communications Security Establishment's Equities Management Framework	CSE	Submitted
21-20—Royal Canadian Mounted Police's Human Source Program	RCMP	Published
22-12—Public Safety and Canadian Security Intelligence Service Accountability Mechanisms	CSIS, GAC, PS, DOJ	Published
23-11—Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2023	PS, CSE, CSIS, GAC, RCMP, CBSA, IRCC	Published

Review	Department(s)	Status**
24-03—Review of Departmental Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2023	CBSA, CSIS, CSE, DND/CAF, GAC, RCMP	Submitted
23-07—Review of the Dissemination of Intelligence on People's Republic of China Political Foreign Interference, 20218-2023	CSIS, RCMP, GAC, CSE, PS, PCO	Published

**Status as of the writing of this report. A review is marked as "Submitted" when the review report has been approved by NSIRA members and sent to the relevant minister(s).

3.2 CSIS Reviews

22-07—Review of the Lifecycle of CSIS's Warranted Information

44. NSIRA examined CSIS's lifecycle management of data resulting from a specific and novel technical capability used to execute a Federal Court warrant. NSIRA inspected CSIS's primary collection and processing system to directly observe how data was collected, processed, and managed.

45. CSIS introduced heightened non-compliance risks when deploying the technical capability with inadequate operational policies and procedures, inadequate data stewardship practices, and inadequate technical systems to handle the resulting data. Consequently, CSIS retained information without a clearly articulated authority.

46. CSIS did not consult with Public Safety Canada as required by the Ministerial Direction prior to using the novel technology under review. CSIS's failure to consult may not have been in compliance with the CSIS Act. CSIS mischaracterized the novel technology as an extension of an existing CSIS technology and failed to inform Public Safety Canada in a timely manner. CSIS did not advise the Federal Court of this novel technology.

47. These shortcomings raised concerns about CSIS's readiness to assess, prepare for and deploy other novel technologies.

Findings	Recommendations	Reviewee's Response
[*Technology*] as a Novel Technology		
Finding 1. NSIRA found that [*technology*] are a novel technology within CSIS's suite of technical capabilities.		
Finding 2. NSIRA found that [*technology*] introduce a significant expansion of collection capabilities and operational risks.		
Finding 3. NSIRA found that CSIS does not have adequate policies and procedures to manage its [*technology*] program.		
Finding 4. NSIRA found CSIS did not consult Public Safety Canada in a timely manner regarding its planned use of [*technology*] contrary to the *Ministerial Direction to the Canadian Security and Intelligence Service on Accountability* issued pursuant to section 6(2) of the CSIS Act. Moreover, CSIS may not be in compliance with section 7(1)(b) of the CSIS	**Recommendation 1.** NSIRA recommends that CSIS establish and maintain adequate policies and procedures to manage its [*technology*] program.	**Agree**

Findings	Recommendations	Reviewee's Response
Act, which requires the Director to consult with the Deputy Minister when required pursuant to Ministerial Direction.		
Data Lifecycle Management		
Finding 5. NSIRA found that CSIS incorrectly labelled some data collected during [*operation*] and no quality assurance or compliance process detected this prior to NSIRA's technical inspection.		
Finding 6. NSIRA found that CSIS retained collected information without clearly articulating the authority for its retention.		
Finding 7. NSIRA found that CSIS does not adequately consider data stewardship requirements accruing from new collection activities, which introduces heightened non-compliance risks.	**Recommendation 2.** NSIRA recommends that CSIS prioritize investing in technical processes and systems that can assess, ingest, label, use, and destroy data in compliance with its legal obligations.	**Agree**
Risk Assessment Practices		

Findings	Recommendations	Reviewee's Response
Finding 8. NSIRA found that CSIS relies on the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* to operationalize the 2019 Ministerial Direction to the Canadian Security Intelligence Service on Accountability. However, the 2020 Framework does not fully capture the requirements of the 2019 Ministerial Direction.	**Recommendation 3.** NSIRA recommends that the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to fully align with the 2019 *Ministerial Direction to the Canadian Security Intelligence Service on Accountability*."	**Agree**
	Recommendation 4. NSIRA recommends that the definition of "novel technique or technology" in the 2020 *Framework for Cooperation Between Public Safety Canada and the Canadian Security Intelligence Service* be revised to err on the side of inclusivity.	**Agree**
	Recommendation 5. NSIRA recommends that CSIS ensure risk assessments performed throughout the lifecycle of new technologies and techniques are rigorous, documented and comprehensive in their scope.	**Agree**
Operational Technology Review Committee (OTRC)		

Findings	Recommendations	Reviewee's Response
Finding 9. NSIRA found that the creation of the Operational Technology Review Committee was an important step forward in CSIS's management of new technologies and techniques.	**Recommendation 6.** NSIRA recommends that, as part of its ongoing development, the Operational Technology Review Committee refine its processes to: • consider data lifecycle requirements; • reference a definition of "novel technology" that has been agreed upon with Public Safety Canada as part of a revised Framework; • include a requirement to consult Public Safety Canada on plans or proposals to seek or develop novel techniques and technologies; • define how risk is assessed; and • better document its technical, legal, foreign policy and reputational risks assessments.	**Agree**
Execution of Warranted Powers		
Finding 10. NSIRA found that, in [*operation*], CSIS intended to [*specific operation details*] beyond warranted targets at a [*location].	**Recommendation 7.** NSIRA recommends that language in the *[*warrant type*] Warrant* more clearly describe the breadth and limitations of what constitutes incidental collection.	**Partially Agree**
	Recommendation 8. NSIRA recommends that CSIS specify the warrant authority in the operational planning documents in support of [*sensitive info*] to be sought in the operation.	**Agree**

Findings	Recommendations	Reviewee's Response
Regulations		
Finding 11. NSIRA found that CSIS's [*use of technology*] may not be in compliance with [*specific*] *Regulations*.		
Duty of Candour		
Finding 12. NSIRA found that CSIS did not advise the Court prior to using [*technology*] in the execution of warranted powers.	**Recommendation 9.** NSIRA recommends that the classified version of this report be shared with the Federal Court.	**Partially Agree**

23-05—Annual Review of Select CSIS Activities (ARSCA-CSIS)

48. In 2024, NSIRA launched a process called the Annual Review of Select CSIS Activities (ARSCA-CSIS). This review covers a range of operational categories which are either routinely communicated to NSIRA by CSIS under a standalone statutory obligation or are of unique interest to NSIRA due to high legal risks or findings of prior reviews. In previous years, NSIRA conducted annual reviews of CSIS Activities that were primarily focused on NSIRA's requirement to report annually to the Minister of Public Safety. However, these reviews did not culminate in a final report with findings and recommendations issued pursuant to section 34 of the NSIRA Act. The work completed this year as part of the ARSCA-CSIS is being captured in a final report with findings and recommendations, thereby aligning with NSIRA's other thematic reviews. The report, which starting this year will be completed annually, will also contain the results of NSIRA's efforts in reviewing an aspect of the CSIS Threat Reduction Regime. The ARSCA-CSIS report that will provide a high-level overview of CSIS activities during the 2024 calendar year has been completed in 2025. Its findings and recommendations will appear in NSIRA's public annual report for the calendar year 2025.

3.3 CSE Reviews

23-02—Annual Review of Select CSE Activities (ARSCA-CSE)

49. In 2024, NSIRA launched a process called the Annual Review of Select CSE Activities (ARSCA-CSE). This review covers a range of operational categories which are either routinely communicated to NSIRA by CSE under a standalone statutory obligation, or are of unique interest to NSIRA due to high legal risks or findings of prior reviews. In previous years, NSIRA conducted Annual Reviews of CSE Activities that were primarily focused on NSIRA's requirement to report annually to the Minister of National Defence. However, these reviews did not culminate in a final report with findings and recommendations issued pursuant to section 34 of the NSIRA Act. The work completed this year as part of the ARSCA-CSE is being captured in a final report with findings and recommendations, thereby aligning with NSIRA's other thematic reviews. The ARSCA-CSE report that will provide a high-level overview of CSE activities during the 2024 calendar year has been completed in 2025. Its findings and recommendations will appear in NSIRA's public annual report for the calendar year 2025.

23-10—CSE's Equities Management Framework

50. NSIRA review of CSE's Equities Management Framework (EMF) resulted in ten findings and seven recommendations that relate to two areas of concern, as well as several shortcomings related to governance and practices. However, at the time of writing, the full report remains heavily classified. As such, more information regarding this review, along with the related findings and recommendations, will be made available at a later date.

3.4 Other Department Reviews

21-20—RCMP's Human Source Program

51. This review was conducted alongside reviews of similar programs at the Canada Border Services Agency and the Department of National Defence/Canadian Armed Forces.

52. NSIRA's review focused on three areas: risk management, duty of care to human sources, and ministerial direction accountability. NSIRA found that risk assessments were inconsistently applied, leading to varied assessments on source suitability. The RCMP was overly reliant on confidentiality promises and failed to fully consider risks to sources. Risk assessments often prioritized investigative outcomes over the safety of informants and lacked proper documentation.

53. Additionally, NSIRA found that the RCMP did not exercise the required "special care" when sources operated in sensitive sectors. There were no mechanisms to assess the cumulative impact of such operations. Anecdotal evidence suggested these practices negatively affected both investigations and Canadian society. In addition, at the time of writing, NSIRA was still awaiting responses from departments to its recommendations.

Findings	Recommendations	Reviewee's Response
	Policy Implementation	

Finding 1. NSIRA found that the RCMP's dated human source policy does not provide a sufficient framework for the consistent application of the Source Development Unit methodology in the proactive recruitment of human sources.	**Recommendation 1.** NSIRA recommends that the RCMP update its human source policy to include, at a minimum:
	• a centralized framework that requires the Human Source Program policy centre to establish:
	  ○ clear thresholds and guidance on the appropriate criteria for the use of proactive recruitment methods in national security investigations,
	  ○ strong oversight and accountability by monitoring and tracking policy compliance; and
	• entrenched methodology principles, including for the	

Findings	Recommendations	Reviewee's Response
	conduct of a standardized approach to the assessment of risk to human sources in all national security investigations.	
Policy Governance — Risk Assessment		
Finding 2. NSIRA found that the risk assessment for agents is adequate because it is comprehensive and details the management of risk as a shared responsibility involving multiple independent stakeholders.		
Finding 3. The risk assessment framework for confidential informants is inadequate. The current assessments of risk: • are not well documented and as such do not provide adequate or reliable information to decision-makers; and • are primarily focused on operational security and risk to the investigation, as opposed to risk to the confidential informants.	**Recommendation 2.** NSIRA recommends that the RCMP revise its risk assessment framework for confidential informants to require officers to consider all applicable risks to the confidential informant, and to aggregate and document those risks, thereby providing for a full accounting.	
Agents — Duty of Care and Informed Consent		

Findings	Recommendations	Reviewee's Response
Finding 4. RCMP's discharge of its duty of care toward agents is satisfactory because the current process: • considers a wide range of risks; • ensures that obligations for informed consent are met; • accounts for risk mitigation measures; • provides for administrative interviews; and • includes independent third party assessments.	**Recommendation 3.** NSIRA recommends that the RCMP adjust the parameters for the conduct of agent interviews so that agent feedback is more descriptive concerning their experience; and documented with greater frequency.	
Confidential Informants — Duty of Care and Informed Consent		
Finding 5. NSIRA found that the RCMP over relies on the promise of confidentiality and does not adequately consider the risk to confidential informants.	**Recommendation 4.** NSIRA recommends that the RCMP improve its risk assessment framework for confidential informants. At a minimum, the framework should: • consider the safety of the confidential informant; • consider the particular circumstances of the confidential informant; • aggregate information that allows for the detection of outstanding vulnerabilities; and • provide for consent from the confidential informant that is	

Findings	Recommendations	Reviewee's Response
	considerate of the risks involved.	
	Recommendation 5. NSIRA recommends that RCMP lower the threshold to conduct administrative interviews so they are conducted with greater regularity and with a greater proportion of confidential informants.	
Ministerial Direction — National Security Investigations in Sensitive Sectors		
Finding 6. NSIRA found that the RCMP has not demonstrated special care in its national security investigations in sensitive sectors, contrary to obligations under the *Ministerial Direction — National Security Investigations in Sensitive Sectors*.		
Finding 7. NSIRA found that the RCMP has an inadequate framework to ensure the appreciation of the cumulative impact of national security investigations in Canadian Fundamental Institutions.	**Recommendation 6.** NSIRA recommends that the RCMP create a specialized Sensitive Sector Unit that is responsible for monitoring and aggregating information on the RCMP's activities as they relate to Canadian Fundamental Institutions, assessing the impact of these activities on the community, and conduct long-term analysis of the cumulative effects.	

3.5 Multi-Departmental Reviews

22-12— Public Safety and Canadian Security Intelligence Service Accountability Mechanisms (CSIS, GAC, PS, DOJ)

54. Following a September 2022 referral by the former Minister of Public Safety (PS), NSIRA reviewed whether CSIS's risk assessment model, Ministerial Direction, and information-sharing mechanisms supported the Minister's discharge of their responsibilities for CSIS.

55. Directions to CSIS coming from political level actors—rather than the Minister or the CSIS Director—during an active operation created unnecessary danger for the CSIS team and caused harm to Canada's international reputation.

56. CSIS and PS failed to provide timely and accurate information to the Minister, which may result from PS's dependence on CSIS to identify and receive relevant information. This would inhibit PS's ability to prepare independent advice to the Minister.

57. Certain Ministerial Directions to CSIS are subject to inconsistent and contradictory interpretation, which affects their implementation. The report raises a number of issues with the pillars of risk evaluated: operational, legal, foreign policy, and reputational.

58. Ultimately, the Minister of Public Safety may not be consistently supported and briefed about pertinent CSIS operations, which raises concerns about the possible erosion of ministerial accountability for the CSIS.

Findings	Recommendations	Reviewee's Response
Accountability and Consequences for Halting the Operation [*codename*]		
Finding 1. NSIRA found that a decision was made to halt an active CSIS operation overseas that was not made by the CSIS Director under section 6(1)	**Recommendation 1.** NSIRA Recommends that whenever there is a decision affecting an active CSIS operation, which is not made by the Director of CSIS or their delegates, it must come as a direction from the	**Agree**

Findings	Recommendations	Reviewee's Response
of the CSIS Act, and for which there is no written record of a direction coming from the Minister of Public Safety under sections 6(1) or 6(2) of the CSIS Act.	Minister of Public Safety under section 6(1) of the CSIS Act and should be accompanied by a written record in keeping with section 6(2).	
Finding 2. NSIRA found that [*political-level actors*] halted an active operation, creating unnecessary danger for the CSIS team [**], and caused harm to Canada's international reputation.		
Responsibility for Briefing the Minister About [*codename*]		
Finding 3. NSIRA found that Public Safety and CSIS failed in their responsibility to provide timely and accurate information to the Minister of Public Safety about [**] human source [**] operation.		
Public Safety's Role in Relation to CSIS		
Finding 4. NSIRA found that Public Safety willingly remains dependent on CSIS to identify and receive relevant information, which inhibits	**Recommendation 2.** NSIRA recommends that the Minister of Public Safety take action to ensure that the Deputy Minister obtains any information required to fulfill their responsibility to provide independent advice to the	**Partially Agree**

Findings	Recommendations	Reviewee's Response
Public Safety's ability to prepare independent advice to the Minister about the activities and operations of CSIS.	Minister about the activities and operations of CSIS.	
	Ministerial Direction to CSIS	
Finding 5. NSIRA found that multiple Ministerial Directions to CSIS are subject to inconsistent and contradictory interpretation by those responsible for their implementation.	**Recommendation 3.** NSIRA recommends that the Minister of Public Safety consolidate ministerial directions into clear, concise and harmonized instruments that are derived from meaningful consultation among those responsible for their implementation.	**Agree**
Finding 6. NSIRA found that when preparing Ministerial Directions to CSIS, Public Safety insufficiently consulted with Global Affairs Canada and CSIS.		
	CSIS's Risk Assessment Process	
Finding 7. NSIRA found that CSIS's risk assessment process has evolved to become the central mechanism for planning operations and managing associated risks, and, while it is generally effective, it lacks clear		

Findings	Recommendations	Reviewee's Response
guidance to employees on when risk should be reassessed as operations evolve.		
Legal Pillar		
Finding 8. NSIRA found that legal advice is often absent from the final risk assessment record for CSIS operations.	**Recommendation 4.** NSIRA recommends that CSIS, in consultation with the Department of Justice and Global Affairs Canada, ensure that legal risk assessments are comprehensive and memorialized in writing.	**Agree**
Finding 9. NSIRA found that the scope of legal considerations within legal risk assessment is under-inclusive.		
Foreign Policy Pillar		
Finding 10. NSIRA found that Global Affairs Canada and CSIS do not have a shared vision with respect to the role of Global Affairs Canada in the foreign policy risk assessment.	**Recommendation 5.** NSIRA recommends that any pending changes to CSIS's risk assessment process maintain a robust consultation and information sharing mechanism between Global Affairs Canada and CSIS.	**Agree**
Reputational Pillar		
Finding 11. NSIRA found that Public Safety is not adequately contributing to the preparation of	**Recommendation 6.** NSIRA recommends that Public Safety and CSIS develop a more robust consultation mechanism for reputational risk assessment for CSIS operational	**Partially Agree**

Findings	Recommendations	Reviewee's Response
reputational risk assessments.	activities, and that these assessments account for the risk of discrediting the Government of Canada.	

23-11— 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, IRCC)

59. The purpose of this review was to determine whether Government of Canada (GC) institutions complied with the *Security of Canada Information Disclosure Act* (SCIDA)'s requirements for disclosure and record keeping in 2023. For the first time in SCIDA's history, NSIRA has found full compliance with the Act, but NSIRA made seven recommendations to mitigate the risks of non-compliance.

60. Albeit compliant with the SCIDA, some IRCC disclosures presented a risk of non-compliance with SCIDA's contribution and proportionality tests. The disclosing institution must be satisfied that both tests are met before making a disclosure under the SCIDA. Yet, four disclosures raised concerns with regard to the amount of personal information that IRCC disclosed.

61. At times, CSIS request letters were unclear, which hindered IRCC's effort to conclude that the disclosure was authorized. The departments are required to provide information on the accuracy and reliability of the manner the disclosed information was obtained. However, NSIRA found that IRCC provided template statements on accuracy and reliability that were not always relevant.

62. CBSA's record of disclosure form contradicts the SCIDA by suggesting that the provision of information on accuracy and reliability is optional.

Findings	Recommendations	Reviewee's Response
Record Keeping Requirements — Section 9		

Findings	Recommendations	Reviewee's Response
Finding 1. NSIRA found that every institution that disclosed or received information pursuant to SCIDA in 2023 complied with their record keeping obligations under section 9, but some records were inaccurate or imprecise.		
Contribution and Proportionality Tests — Subsection 5(1)		
Finding 2. NSIRA found, within the sample of disclosures reviewed that disclosing institutions demonstrated they had satisfied themselves under the contribution and proportionality tests in compliance with subsection 5(1) of the SCIDA.	**Recommendation 1.** 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.	**Agree**
Finding 3. NSIRA found that IRCC did not, in one instance, independently consider whether its disclosure related to activities that fell under the SCIDA exception for advocacy, protest, or dissent. Instead, IRCC satisfied itself of the SCIDA's contribution test based on assumptions about how CSIS assessed activities that undermine the security of Canada.	**Recommendation 2.** NSIRA recommends that IRCC amend their SCIDA policy to underscore that IRCC must independently assess whether the disclosure is authorized. This assessment should consider whether the activity amounts to one of the exceptions to the SCIDA's definition of activities that undermine the security of Canada.	**Agree**
Finding 4. NSIRA found that, throughout the course of 2023, IRCC improved the rigour of its proportionality assessments regarding disclosure of passport	**Recommendation 3.** NSIRA recommends that IRCC apply an iterative approach to its proportionality assessments, with a view to disclosing only the minimum	**Agree**

Findings	Recommendations	Reviewee's Response
information. However, NSIRA identified three instances where IRCC disclosed visa information without applying the same rigorous approach, which risked disclosing more personal information than reasonably necessary in the circumstances.	information reasonably necessary in the circumstances to enable the recipient institution to further their investigation.	
Finding 5. NSIRA found that CSIS requests to IRCC used inconsistent terminology and were often unclear about the relationship between the subject of the request and its investigation. At times, this lack of clear communication hindered IRCC's efforts to satisfy itself that the disclosure was authorized under the SCIDA.	**Recommendation 4.** NSIRA recommends that CSIS use consistent terminology, and be clear about the nature of the link that has been established between the subject of a request and its investigation, to assist IRCC in satisfying itself of the proportionality test.	**Agree**
Reliability and Accuracy Statement — Subsection 5(2)		
Finding 6. NSIRA found that disclosing institutions provided information regarding the accuracy of the information and reliability of the manner in which it was obtained in relation to all disclosures. However, CBSA made one verbal disclosure that did not include an explicit statement on accuracy and reliability.	**Recommendation 5.** NSIRA recommends that institutions avoid making verbal disclosures whenever possible. When they must occur, verbal disclosures should explicitly convey the requisite information on accuracy and reliability.	**Agree**
Finding 7. NSIRA found that CBSA's record of disclosure form	**Recommendation 6.** NSIRA recommends that CBSA harmonize	**Agree**

Findings	Recommendations	Reviewee's Response
contradicts the SCIDA by allowing officials to opt out of providing information regarding accuracy and reliability.	its record of disclosure form with the SCIDA, to convey the mandatory nature of providing information on accuracy and reliability at the time of the disclosure.	
Finding 8. NSIRA found that IRCC used "templated" language to describe the disclosure's accuracy and reliability that was not always relevant or specific to the circumstances of the disclosure.	**Recommendation 7.** NSIRA recommends that IRCC tailor its statements on accuracy and reliability as to ensure that each disclosure's statement is specific to the circumstances of the case.	**Agree**
Information Sharing Agreement — Subsection 4(c)		
Finding 9. NSIRA found that disclosures between IRCC and CSE that occurred following the enactment of their new information sharing agreement were compliant with both the SCIDA and their information-sharing agreement.		

24-03—Review of Departmental Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2023: Mitigation and Armed Conflict (CBSA, CSIS, CSE, DND/CAF, GAC, RCMP)

63. 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 (ACA Directions) during the 2023 calendar year. It focused on how departments mitigated a substantial risk of mistreatment when sharing information with foreign entities.

64. NSIRA reviewed a number of cases concerning disclosures to foreign entities engaged in armed conflict and considered how armed conflict affected departments' ability to mitigate.

65. Three departments that shared with foreign entities engaged in armed conflict may not have been compliant with the ACA Directions.

66. A foreign country's involvement in armed conflict created challenges for departments in meeting their mitigation obligations under the ACA Directions. NSIRA further observed challenges related to disclosures contemplated to serve humanitarian objectives. NSIRA noted that the circumstances of armed conflict left few options for departments pursuing humanitarian objectives to mitigate the risks resulting from sharing.

67. NSIRA directed departments to conduct a study of information-sharing with the foreign entities of countries engaged in armed conflict to analyze challenges in compliance with the ACA Directions and gaps in the ACA regime. In addition, at the time of writing, NSIRA was still awaiting responses from departments to its recommendations.

Findings	Recommendations	Reviewee's Response
Finding 1. NSIRA found that, in the cases examined, CSIS, GAC, RCMP, and IRCC's mitigation determinations demonstrated common deficiencies, including: • inadequate design of mitigation measures to address the specific risks of mistreatment present; • insufficient assessment of caveats and assurances for clarity and reliability; and • improper incorporation of external considerations into the determinations of whether a substantial risk of	**Recommendation 1.** NSIRA recommends that departmental ACA risk assessments include thorough mitigation plans wherever a substantial risk of mistreatment is identified. These plans should: • consider whether all mitigation measures proposed, taken globally, adequately address the specific risks alive in the case at issue and are capable of sufficiently lessening those risks; • evaluate the reliability of any caveats and assurances proposed and weigh histories of	

Findings	Recommendations	Reviewee's Response
mistreatment could be mitigated. **Finding 2.** NSIRA found that, in the case examined, CSIS may not have been in compliance with the ACA Directions, as they were unlikely to have sufficiently mitigated a substantial risk of mistreatment when sharing information with a foreign entity. Specifically, CSIS: • relied upon caveats and assurances that were inadequately designed to address the specific risks of mistreatment present; and • did not resolve substantial deficiencies that undermined the reliability of the caveats and assurances. **Finding 3.** NSIRA found that, in the case examined, GAC's poor record-keeping practices impeded NSIRA's ability to determine their compliance with the ACA Directions. **Finding 4.** NSIRA found that, in the case examined, the RCMP may not have been in compliance with the ACA Directions, as they	compliance according to their quality; • exclude any external considerations that are not relevant to the question of mitigation, including the risk of not sharing, and strategic or reputational considerations; and • include a plan to monitor for indications of mistreatment and adherence to caveats and assurances following an information exchange.	

Findings	Recommendations	Reviewee's Response
were unlikely to have sufficiently mitigated a substantial risk of mistreatment when sharing information with a foreign entity. Specifically, the RCMP relied upon caveats that were inadequately designed to address the specific risks of mistreatment present. **Finding 5.** NSIRA found that, in the case examined, IRCC may not have been in compliance with the ACA Directions, as they were unlikely to have sufficiently mitigated a substantial risk of mistreatment when sharing information with a foreign entity. Specifically, IRCC relied upon measures that were inadequately designed to address the specific risks of mistreatment present. **Finding 6.** NSIRA found that many of DND/CAF's mitigation practices served to provide decision-makers with information necessary to determine whether a substantial risk of mistreatment could be mitigated.		

Findings	Recommendations	Reviewee's Response
Finding 7. NSIRA found that a foreign country's involvement in armed conflict created challenges for departments in meeting their mitigation obligations under the ACA Directions when seeking to share information with that country's entities. **Finding 8.** NSIRA found that the practical realities of compliance with the ACA Directions can, in certain circumstances, create a dilemma for departments seeking to share for humanitarian purposes.	**Recommendation 2**. NSIRA recommends that officials clearly document how each identified risk was mitigated prior to disclosing information to foreign entities.	

23-07—Review of the Dissemination of Intelligence on People's Republic of China Political Foreign Interference, 2018–2023 (CSIS, RCMP, GAC, CSE, PS, PCO)

68. This review evaluated processes regarding how collected information was shared and escalated to relevant decision-makers, and indicated that there were significant disagreements in the national security and intelligence community as to whether, when, and how to share relevant information.

69. Three basic schisms existed: CSIS struggled to reconcile competing imperatives given the unique sensitivities of political foreign interference; the Security and Intelligence Threats to Elections (SITE) Task Force and the Critical Election Incident Public Protocol (CEIPP) Panel were geared toward broad, systematic interference and therefore could not adequately address riding-by-riding interference. PCO and

CSIS analysts produced overviews of what they considered to be PRC foreign interference activities, but which the Prime Minister's National Security and Intelligence Advisor (NSIA) saw as recounting standard diplomatic activity.

70. This challenging situation prompts us to ask how to address the so-called grey zone whereby political foreign interference may stand in close proximity to typical political or diplomatic activity. NSIRA saw evidence of this challenge across the activities under review. NSIRA's eight recommendations address these deficiencies. In addition, at the time of writing, NSIRA was still awaiting responses from departments to its recommendations.

Findings	Recommendations	Reviewee's Response
CSIS's Collection and Dissemination of Intelligence on PRC Foreign Interference in the 2019 and 2021 Federal Elections		
Finding 1. NSIRA found that CSIS's dissemination of intelligence on political foreign interference during the 43rd and 44th federal elections was inconsistent. Specifically, in certain instances: • the rationale for decisions regarding whether, when, and how to disseminate intelligence was not clear, directly affecting the flow of information; and • the threat posed by political foreign interference activities was not clearly communicated by CSIS.		
Finding 2. NSIRA found that CSIS's dissemination and use of intelligence on political foreign interference were		

Findings	Recommendations	Reviewee's Response
impacted by the concern that such actions could interfere, or be seen to interfere, in the democratic process.		
Finding 3. NSIRA found that CSIS often elected to provide verbal briefings as opposed to written products in disseminating intelligence on political foreign interference during elections.		
Finding 4. NSIRA found that there was a disconnect within CSIS between a region and National Headquarters as to whether reporting on political foreign interference was subject to higher thresholds of confidence, corroboration and contextualization for dissemination.	**Recommendation 1.** NSIRA recommends that CSIS develop, in consultation with relevant government stakeholders, a comprehensive policy governing its engagement with threats related to political foreign interference. This policy should: • make explicit CSIS's thresholds and practices for the communication and dissemination of intelligence regarding political foreign interference. This would include the relevant levels of confidence, corroboration, contextualization and characterization necessary for intelligence to be reported; • clearly articulate CSIS's risk tolerance for taking action	

Findings	Recommendations	Reviewee's Response
	against threats of political foreign interference; • establish clear approval and notification processes (including external consultations) for all activities related to countering political foreign interference; • make clear any special requirements or procedures that would apply during election/writ periods, as necessary, including in particular procedures for the timely dissemination of intelligence about political foreign interference; and • consider best practices from international partners (in particular the Five Eyes) regarding investigating and reporting about political foreign interference.	
The SITE Task Force and the CEIPP Panel		
Finding 5. NSIRA found that the SITE Task Force and the CEIPP Panel were not adequately designed to address traditional, human-based foreign interference. Specifically: • the SITE Task Force focuses on threat activities during the election period, but traditional foreign	**Recommendation 2.** NSIRA recommends that the SITE Task Force align its priorities with the threat landscape, including threats which occur outside of the immediate election period.	

Findings	Recommendations	Reviewee's Response
interference also occurs between elections; • Global Affairs Canada's representation on the SITE Task Force focused on online foreign interference activities; and • the CEIPP Panel's high threshold for a public announcement is unlikely to be triggered by traditional foreign interference, which typically targets specific ridings.		
	Recommendation 3. NSIRA recommends that Global Affairs Canada (GAC) and the Privy Council Office ensure that GAC's representation on the SITE Task Force leverages the department's capacity to analyze and address traditional, human-based foreign interference, in addition to the online remit of the Rapid Response Mechanism Team.	
	Recommendation 4. NSIRA recommends that the Privy Council Office empower the CEIPP Panel to develop additional strategies to address the full threat landscape during election periods, including when threats manifest in specific ridings.	

Findings	Recommendations	Reviewee's Response
The Flow of Intelligence on PRC Foreign Interference		
Finding 6. NSIRA found that the limited distribution of some CSIS and CSE intelligence to senior officials only reduced the ability of the Royal Canadian Mounted Police, Global Affairs Canada, and the Privy Council Office to incorporate that intelligence into their analysis.		
Finding 7. NSIRA found that CSIS and Public Safety did not have a system for tracking who received and read specific intelligence products, creating unacceptable gaps in accountability.	**Recommendation 5.** NSIRA recommends that, as a basic accountability mechanism, CSIS and Public Safety rigorously track and document who has received intelligence products. In the case of highly sensitive and urgent intelligence, this should include documenting who has read intelligence products.	
Finding 8. NSIRA found that the dissemination of intelligence on political foreign interference from 2018 to 2023 suffered from multiple issues. Specifically: • intelligence consumers did not always understand the significance of the intelligence they received nor how to integrate it into their policy analysis and decision-making;	**Recommendation 6.** NSIRA recommends that Public Safety Canada, Global Affairs Canada, the Privy Council Office, and other regular consumers of intelligence, enhance intelligence literacy within their departments.	

Findings	Recommendations	Reviewee's Response
• there was disagreement between intelligence units and senior public servants as to whether activities described in specific intelligence products constituted foreign interference or legitimate diplomatic activity.		
Finding 9. NSIRA found that there was disagreement between senior public servants and the NSIA as to whether intelligence assessments should be shared with the political executive. Ultimately, the NSIA's interventions resulted in two products not reaching the political executive, including the Prime Minister.	**Recommendation 7.** NSIRA recommends that the security and intelligence community develop a common, working understanding of political foreign interference.	
Finding 10. NSIRA found that the NSIA's role in decisions regarding the dissemination of CSIS intelligence products is unclear.	**Recommendation 8.** NSIRA recommends that the role of the National Security and Intelligence Advisor to the Prime Minister, including with respect to decisions regarding the dissemination of intelligence, be described in a legal instrument.	

04 //

Complaint Investigations

4.1 Overview

71. NSIRA is responsible for investigating complaints from members of the public related to national security. These investigations are carried out with consistency, fairness, and timeliness.

72. NSIRA's jurisdiction covers complaints regarding activities conducted by CSIS or CSE, national security-related complaints against the RCMP, complaints in relations to security clearance denials and, referrals from the Canadian Human Rights Commission (CHRC) or under the *Citizenship Act*.

73. In 2024, NSIRA continued to investigate a wide range of complaints from previous years, successfully bringing several to a conclusion. NSIRA also initiated many new investigations, including with respect to a large increase in public complaints against CSIS regarding immigration and citizenship security screening, as detailed further below.

74. Finally, NSIRA continues to implement several initiatives aimed at enhancing and streamlining its processes and procedures.

Increase of complaints against CSIS regarding delays in immigration or citizenship security screening

75. From August to December 2024, NSIRA observed a significant increase of complaints against CSIS filed pursuant to section 16 of the NSIRA Act, alleging process delays in immigration or citizenship security screening. Out of 79 complaints received pursuant to s.16 of the NSIRA Act in 2024, 52 (66%) related to such delays. Of note, under ss. 14 and 15 of the CSIS Act, CSIS provides security advice to IRCC and CBSA regarding immigration or citizenship applicants. CSIS has advised NSIRA that the time it takes to provide security advice is influenced by several factors, including the prioritization of files, resource limitations, and priorities established by the Government of Canada, such as special immigration measures and humanitarian initiatives in response to crises around the world.

76. As depicted by the statistics found at the end of the current section, several of these complaints have resulted in informal resolutions. More specifically, upon completion of CSIS's security screening of a complainant's citizenship or immigration application, CSIS provides a letter that can be shared with the complainant which indicates that the advice has been provided to the requesting client, and that CSIS's role is now complete. The complainant may then elect to continue with their complaint or informally resolve it.

4.2 Ongoing Initiatives

77. NSIRA's Rules of Procedure govern the process for complaint investigations. While respecting the classified nature of the proceedings, they ensure that parties have the fullest opportunity to participate and make representations, and that all proceedings are conducted as informally and expeditiously as possible.

78. In 2024, NSIRA continued its internal review of the Rules of Procedure to identify issues and develop proposals for future revisions. The review aims to ensure that all investigations remain accessible, efficient, and procedurally fair.

79. Specifically, NSIRA also created a new rule on accessibility and accommodations. The rule will enable NSIRA to meet its commitment to identify, remove, and prevent barriers to accessibility to the greatest extent possible. This will help to ensure that those with disabilities can continue to fully participate in the complaint investigation process.

80. NSIRA also began developing another new rule to create a streamlined process for simplified investigations of non-complex complaints.

4.3 Investigation Report Summaries

Final Reports Issued

Harassment allegations against the Royal Canadian Mounted Police
(NSIRA File 07-407-13)

81. The Complainant alleged that RCMP members had shown up unannounced and without a warrant at their home. The Complainant alleged harassment by the said RCMP members during that unexpected visit. The RCMP members went to the

Complainant's home following an anonymous report, according to which the Complainant had made threats against the Prime Minister.

82. The interaction between the RCMP members and the Complainant was filmed by the bodycam worn by a municipal police officer. The video was submitted as evidence by the RMCP in the NSIRA investigation.

83. Following a review of the documentary evidence submitted by the RCMP and the Complainant, as well as an investigative interview with the latter, NSIRA found that under the implicit invitation provided by Common Law, the RCMP members had the right to go unannounced and without a warrant to the Complainant's house to have a discussion with the said Complainant. The purpose of the RCMP members' visit was to determine whether the Complainant posed a threat to the public and to the Prime Minister, not to substantiate any accusations against the said Complainant or to make an arrest.

84. NSIRA also found that the RCMP members had not harassed the Complainant during the interaction.

85. NSIRA found the Complainant's allegations to be unsubstantiated.

Allegations against the Department of National Defence for denial of Top Secret security clearance and revocation of reliability status (NSIRA File 07-404-30)

86. The Complainant alleged that, based on their voluntary disclosure during security interviews, they were denied a Top Secret security clearance and had their reliability status revoked, which resulted in their release from the Canadian Forces. NSIRA found that it had no jurisdiction to make findings and recommendations regarding revocation of reliability status and confined its discussion to matters implicating the security clearance decision only.

87. The Complainant alleged that the Vice Chief of the Defence Staff's (VCDS) security clearance decision was flawed for several reasons, including that the Complainant's sexuality influenced the VCDS decision; the VCDS did not take into account the Complainant's mental health situation and failed to inquire about a mental health nexus in their case and provide accommodation; the decision did not meet DND's security screening standards; the decision was inconsistent with the recommendation offered by the Complainant's commanding officer; and the decision did not acknowledge a number of considerations that might mitigate the seriousness of the adverse information against the Complainant.

88. NSIRA found the Complainant's allegations to be unsubstantiated. Specifically, NSIRA found that the VCDS decision was not motivated by a concern or consideration of the Complainant's sexuality or sexual orientation; that in the circumstances, no duty to accommodate was triggered for the purposes of the VCDS decision based on the Complainants mental health situation; that were unsubstantiated the allegations that the VCDS failed to meet security screening standards and that DND failed to properly review the surrounding circumstances; that the assertion that the VCDS decision was improper because it was inconsistent with the Complainant's commanding officer's recommendation was unsubstantiated; and that the Complainant's other allegations, including those with respect to considerations that might mitigate the seriousness of the adverse information against them, did not individually or collectively render the decision unreasonable. In addition, NSIRA found no violation of procedural fairness.

89. However, NSIRA observed that certain exculpatory information was excluded from the Threat and Risk Assessment (TRA) before the decision-maker and recommended that this practice be rectified in the future. However, this omission did not amount to a breach of procedural fairness in the circumstances.

Allegations against CSIS for racial profiling, interrogation and harassment, information-sharing with foreign agencies, travel difficulties, and citizenship issues (NSIRA File 07-403-05)

90. The Complainant alleged that CSIS had been racially profiling them; that CSIS agents harassed and interrogated them on multiple occasions; that CSIS shared information about them with foreign countries, leading to them having travel difficulties; that CSIS was responsible for their travel difficulties; and that CSIS put their citizenship application on hold.

91. SIRC took jurisdiction of this complaint in 2018, and when NSIRA came into force in 2019, this investigation was deemed to be continued before NSIRA.

92. In the investigative report, NSIRA provided clarity on the standard of review in section 16 complaints — namely, that NSIRA is charged with making findings and recommendations with respect to legality, reasonableness, and necessity in the exercise of CSIS's powers. In gauging reasonableness and necessity, the Member adopted an objective standard: would a reasonable person charged with exercising CSIS's mandates and apprised fully of the facts, as were available to CSIS, conclude that CSIS's exercise of its powers was necessary and proportional?

93. On the facts of this investigation, NSIRA found that the allegations were unsubstantiated, but made several recommendations. The recommendations addressed observations concerning how CSIS manages the aftermath of section 12 investigations and the circumstances in which CSIS should retract or correct information that it shared with foreign agencies.

Allegations against CSIS for conspiracy, electronic surveillance, travel difficulties, information sharing, and unlawful conduct (NSIRA File 07-403-69)

94. The Complainant alleged that CSIS directed an unlawful seizure of their property in 2011; unlawfully shared information with Canadian and foreign authorities; conspired with government departments; harassed, surveilled, targeted, and intercepted their phone calls; acted unlawfully and breached their human or Charter rights. In addition, the Complainant alleged that they had issues re-entering Canada after the impugned seizure took place due to CSIS's activities. NSIRA found that the allegations were unsubstantiated.

Allegations against CSE for breach of consent and procedural fairness as part of security screening and hiring processes (NSIRA File 07-406-04)

95. The Complainant alleged that, as part of their security screening and hiring processes at CSE, CSE breached their consent and procedural fairness; squandered government resources; failed to use approved security screening tools that have been approved by TBS and undergone the required Privacy Impact Assessment; received verbal disclosures or slander from the Complainant's former employer regarding their character; harassed them; denied them a security clearance; and cited suitability concerns as a technique to circumvent NSIRA's jurisdiction under section 18 of the NSIRA Act with respect to complaints related to denials of security clearances.

96. NSIRA concluded that the Complainant's first allegation that CSE had breached their consent, and more specifically that CSE improperly used information the Complainant disclosed during their security interview for human resources and suitability purposes, was supported. The consent form signed by the Complainant in preparation for the security interview only contemplated the collection of information for the purpose of obtaining a security clearance. The evidence before NSIRA revealed that the Complainant was not advised prior to the security interview that the information collected could have been subsequently used for

other purposes, including to assess their suitability for employment. Accordingly, NSIRA found that CSE had not complied with section 7 of the *Privacy Act*.

97. With respect to the Complainant's remaining allegations against CSE, NSIRA found that they were unsubstantiated by the evidence.

98. In its Final Report, NSIRA issued two recommendations:

- That CSE review the consent form that is presented to and signed by candidates prior to a security interview as part of the security screening process, and amend it accordingly; and
- That CSE consider undertaking a Privacy Impact Assessment of its security interview questionnaire if one has not been conducted yet.

Allegations against CSIS for racism/racial profiling, harassment, slander, information-sharing with foreign agencies, travel difficulties (NSIRA File 07-403-12)

99. The Complainant alleged that CSIS subjected them to harassment, racial profiling, and slander. The Complainant suggests that they were targeted because of their racial or ethnic background, legitimate political opinions, and due to their work as a confidential police informant. They suggested that, due to CSIS's conduct, they had social, psychological and financial hardship, and difficulty travelling.

100. SIRC took jurisdiction of this complaint in January 2019, and when NSIRA came into force in July 2019, this investigation was deemed to be continued before NSIRA.

101. NSIRA found the Complainant's allegations to be unsubstantiated. Specifically, it found that CSIS did not unlawfully investigate the Complainant or engage in racial profiling; did not target the Complainant because of their activities as a confidential police informant; did not slander or defame the Complainant, damage their reputation or sabotage their relationships; did not harass the Complainant or conduct interviews with them in an unlawful or unreasonable manner; did not unlawfully or unreasonably share information about the Complainant with foreign agencies or collude with them to interfere with their travel; did not breach the Complainant's privacy rights under the Charter; and did not unlawfully retain personal information.

4.4 Other Outcomes

Allegations against CSIS's role in delaying security assessment regarding immigration or citizenship applications (NSIRA Files 07-403-98, 07-403-100, 07-403-101, 07-403-105, 07-403-106, 07-403-110, 07-403-113, 07-403-118, 07-403-124, 07-403-125, 07-403-126, 07-403-127, 07-403-129, 07-403-131, 07-403-132, 07-403-133, 07-403-135, 07-403-136, 07-403-151, 07-403-155)

102. A number of Complainants filed complaints against CSIS alleging that CSIS caused a significant delay in providing security screening advice for their immigration or citizenship applications. CSIS provided letters to NSIRA that could be shared with the Complainants advising them that CSIS had provided its advice to the requesting client and that CSIS's role in the security screening process was complete. As the Complainants' main allegations against CSIS were in relation to the delay in the security screening, NSIRA inquired with the Complainants as to whether they wished to resolve their complaints in light of the update received. In the above-referenced files, the Complainants informed NSIRA that they did not wish to proceed with an investigation into their respective complaints against CSIS. As such, the matters were informally resolved in accordance with Rule 10.10 of NSIRA's *Rules of Procedure* or withdrawn.

Deemed abandonment of complaint against a government department for denial of security clearance resulting rescinded job offer (NSIRA File 07-404-25)

103. The Complainant alleged that, after being offered employment by a Government of Canada department conditional upon obtaining a Reliability and Secret clearance, they were denied said clearance because of a residency issue. The Complainant alleged that this was an inaccurate application of clearance policies, and that the employment offer was rescinded after the Complainant indicated that they would pursue the matter further.

104. NSIRA found the complaint to be deemed abandoned according to Rule 15.02 of NSIRA's Rules of Procedure, following its reasonable attempts to communicate with the Complainant who refrained from participating in the process.

Informal resolution of a complaint regarding the denial of a security clearance
(NSIRA File 07-404-37)

105. The Complainant alleged that they were denied employment with an agency in the Government of Canada due to the denial of the required Top Secret security clearance. The Complaint alleged that the decision was based on inaccurate information and that the agency disregarded exculpatory information that the Complainant provided to correct the inaccuracies. The Complainant also alleged that they had a pending Secret security clearance application with another department that was unreasonably delayed.

106. Following an informal resolution meeting facilitated by NSIRA and attended by the Complainant and responding government agency, the parties asked NSIRA to place the investigation into abeyance pending the outcome of the Complainant's Secret security clearance application. NSIRA granted the request. The Complainant subsequently informed NSIRA that they received their Secret security clearance and no longer wished to proceed with the complaint. NSIRA accepted the informal resolution.

4.5 Statistics on Complaint Investigations

January 1, 2024, to December 31, 2024

Intake Inquiries	142
New complaints filed	79
NSIRA Act, section 16, Canadian Security and Intelligence Service (CSIS) complaints	67
NSIRA Act, section 17, Communication Security Establishment (CSE) complaints	2
NSIRA Act, section 18, Security clearances	0
NSIRA Act, section 19, Royal Canadian Mounted Police (RCMP) referred complaints	10
Citizenship Act, section 19	0

Canadian Human Rights Act, section 45 (CHRC referrals)			0
Decision on jurisdiction to investigate			
	Accepted	**Declined**	**Withdrawn**
NSIRA Act, section 16 (CSIS complaints)	22	10	7
NSIRA Act, section 17 (CSE complaints)	0	3	0
NSIRA Act, section 18 (security clearances)	0	2	0
NSIRA Act, section 19 (RCMP referred complaints)	3	2	0
Total	25	17	7
Active investigations as of December 31, 2024			34
NSIRA Act, section 16 (CSIS complaints)			23
NSIRA Act, section 17 (CSE complaints)			0
NSIRA Act, section 18 (Security clearances)			4
NSIRA Act, section 19 (RCMP referred complaints)			7
Canadian Human Rights Act, section 45 (CHRC referrals)			0

Informal resolution in progress as of December 31, 2024				2
NSIRA Act, section 16 (CSIS complaints)				2
NSIRA Act, section 17 (CSE complaints)				0
NSIRA Act, section 18 (security clearances)				0
NSIRA Act, section 19 (RCMP referred complaints)				0
Canadian Human Rights Act, section 45 (CHRC referrals)				0
Total investigations closed				22
	Abandoned	**Final report**	**Resolved informally**	**Withdrawn**
NSIRA Act, section 16 (CSIS complaints)	0	3	14	0
NSIRA Act, section 17 (CSE complaints)	0	1	0	0
NSIRA Act, section 18 (security clearances)	1	1	1	0
NSIRA Act, section 19 (RCMP referred complaints)	0	1	0	0
Canadian Human Rights Act, section 45 (CHRC referrals)	0	0	0	0
Total	1	6	15	0
Investigations carried to the next calendar year				34
NSIRA Act, section 16 (CSIS complaints)				23
NSIRA Act, section 17 (CSE complaints)				
NSIRA Act, section 18 (security clearances)				4
NSIRA Act, section 19 (RCMP referred complaints)				7

Canadian Human Rights Act, section 45 (CHRC referrals)	0

Note: Abbreviations are spelled out in Annex A.

05 //

Looking Ahead

5.1 Advancing NSIRA's Vision

107. NSIRA's vision — an accountable, transparent, and effective national security and intelligence community that upholds the rule of law — has guided every aspect of the Review Agency's work in 2024. Through expanded transparency initiatives, timely public reporting, and continuous methodological refinement, NSIRA has demonstrated its commitment to achieving this vision. Whether through public-facing communications, the release of unclassified/redacted materials, or the ongoing enhancement of its website, NSIRA has remained focused on building public trust.

108. With the finalization of its 2024-2027 Strategic Plan, NSIRA has established a clear framework for advancing its mandate in the years ahead. The coming year will focus on strengthening the Review Agency's core activities by enhancing review capacity and output, deepening subject-matter expertise, and expanding on the agility of complaint investigations.

109. Guided by its strategic priorities, NSIRA will place greater emphasis on proactive engagement. This includes increased outreach to the media, academic, civil society, parliamentarians, and domestic oversight bodies such as Agents of Parliament. NSIRA also aims to strengthen its relationships with international counterparts to continue sharing best practices and contribute to global efforts in national security accountability. These initiatives will support NSIRA's continued evolution as a modern, transparent, and effective review body well positioned to meet the challenges of 2025 and beyond.

06 //

Annexes

Annex A: Abbreviations

Abbreviation	Full Name
ACA	*Avoiding Complicity in Mistreatment by Foreign Entities Act*
ARSCA-CSE	Annual Review of Select CSE Activities
ARSCA-CSIS	Annual Review of Select CSIS Activities
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CEIPP	Critical Election Incident Public Protocol
CHRC	Canadian Human Rights Commission
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
FIORC	Five Eyes Intelligence Oversight and Review Council
GAC	Global Affairs Canada
IRCC	Immigration, Refugees and Citizenship Canada
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
OPC	Office of the Privacy Commissioner of Canada
PCO	Privy Council Office
PS	Public Safety
RCMP	Royal Canadian Mounted Police

SCIDA	*Security of Canada Information Disclosure Act*
SIGINT	Signals Intelligence
SITE	Security and Intelligence Threats to Elections
TRA	Threat and risk assessment
TRM	Threat reduction measure
VCDS	Vice Chief of the Defence Staff

Annex B: Statistics and Data

1. The statistics and data below are provided as per NSIRA's historical practice of including general data received annually from CSIS and CSE. NSIRA has not independently verified or assessed the numbers. Starting next year, such statistical data will be reproduced with the value added of NSIRA analysis and commentary as part of the summaries of the ARSCA-CSIS and ARSCA-CSE review reports.

CSIS Statistics and Data

	2019	2020	2021	2022	2023	2024
Total Warrant Applications	24	15	31	28	30	28
Total Warrants issued by the Court	23	15	31	28	30	27
New Warrants	9	2	13	6	9	5
Replacements	12	8	14	14	10	13
Supplemental	2	5	4	8	11	9
Total Denied Warrants	1	0	0	0	0	1

Source: CSIS (NSIRA did not independently verify these numbers)
Note: The warrant statistics found here represent the total number of warrant applications made to the Federal Court, independent of the actual number of warrants granted in each application or the number of individuals who were the subject of warrants.

Total Number of Approved and Executed Threat Reduction Measures 2019–2024

	2019	2020	2021	2022	2023	2024
Approved TRMs	24	11	23	16	14	11
Executed TRMs	19	8	17	12	19	15
Warranted TRMs	0	0	0	0	0	1

Source: CSIS (NSIRA independently verified these numbers)

Total Number of CSIS Targets, 2019–2024

	2019	2020	2021	2022	2023	2024
Number of Targets	467	360	352	340	323	389
Source: CSIS (NSIRA did not independently verify these numbers)						

Evaluation and Retention of Publicly Available, Canadian, and Foreign Datasets by CSIS, 2019-2024

	2019	2020	2021	2022	2023	2024
Publicly Available Datasets						
Evaluated	9	6	4	4	2	2
Retained	9	6	2	4	2	2
Canadian Datasets						
Evaluated	0	0	2	0	1	0
Retained	0	0	0	2	0	0
Foreign Datasets						
Evaluated	10	0	0	2	1	2
Retained	0	1	1	1	3	4

Source: CSIS (NSIRA did not independently verify this information).

Note: Datasets collected and evaluated in one year may receive ministerial, judicial or other authorization in subsequent years. In addition, datasets may be retained for multiple years as per the CSIS Act.

Authorizations, Commissions, and Directions Under CSIS's Justification Framework, 2019-2024

	2019	2020	2021	2022	2023	2024
Commissions by employees	1	39	51	61	47	34
Authorizations	49	147	178	172	172	175
Directions to Commit	15	84	116	131	116	128
Emergency Designations	0	0	0	0	0	0
Source: CSIS						

Total Number of Non-Compliance Incidents Processed by CSIS, 2019-2024

Incidents	2019	2020	2021	2022	2023	2024
Processed incidents						
Administrative	-	53	64	42	48	54
Operational[1]	40[2]	19	21	17	31	28
Total	53	99	85	59	79	82
Breakdown of Non-compliance (all categories counted)						
Canadian Law	-	-	1	2	4	5
CSIS Act	-	-	-	-	-	3
Charter	-	-	6	5	15	14
Warrant Conditions	-	-	6	3	11	13
CSIS Governance	-	-	8	15	27	25

Source: CSIS

Note: According to CSIS, each compliance instance was factored in all the categories in which it was non-compliant. As a result, the sum of instances may exceed the total number.

[1] 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.

[2] The total number of incidents of non-compliance was 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.

CSE Statistics and Data

Ministerial Authorizations

Name of ministerial authorization	Enabling section of CSE Act	Number of Authorizations Issued in 2024
Foreign Intelligence Authorization	26(1)	3
Cybersecurity Authorization for Federal and Non-Federal Infrastructures	27(1) and 27(2)	4
Defensive Cyberoperations Authorization	29(1)	1
Active Cyberoperations Authorization	30(1)	3
Source: CSE (NSIRA did not independently verify these numbers)		

Ministerial authorizations issued in 2024

Ministerial Orders

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
Source: CSE (NSIRA did not independently verify these numbers)	

Ministerial orders in effect in 2024

Canadian Identifying Information

Type of request	Number of requests received
Government of Canada requests	909
Five Eyes requests	78
Non-Five Eyes requests	6
Total	993
Source: CSE (NSIRA did not independently verify these numbers)	

Requests for disclosure of Canadian Identifying Information related to FI, 2024

Disclosure type	Number of requests
Victim notifications	2,221
Disclosure to partners	9
Total	2,230
Source: CSE (NSIRA did not independently verify these numbers)	

Disclosures of Canadian Identifying Information related to Cybersecurity, 2024

Privacy Incidents

Type of incident	2024
Privacy incidents	75
Second-party privacy incidents	44
Non-privacy compliance incidents	13
Source: CSE (NSIRA did not independently verify these numbers)	

Privacy and non-privacy compliance incidents related to CSE's FI mandate, 2024

Type of incident	2024
Privacy incidents	31
Non-privacy compliance incidents	9
Source: CSE (NSIRA did not independently verify these numbers)	

Privacy and non-privacy compliance incidents related to CSE's Cybersecurity mandate, 2024

Technical and Operational Assistance

Received	Approved	Denied	Cancelled
48	49	2	2
Source: CSE (NSIRA did not independently verify these numbers)			

Requests for technical and operational assistance, 2024.