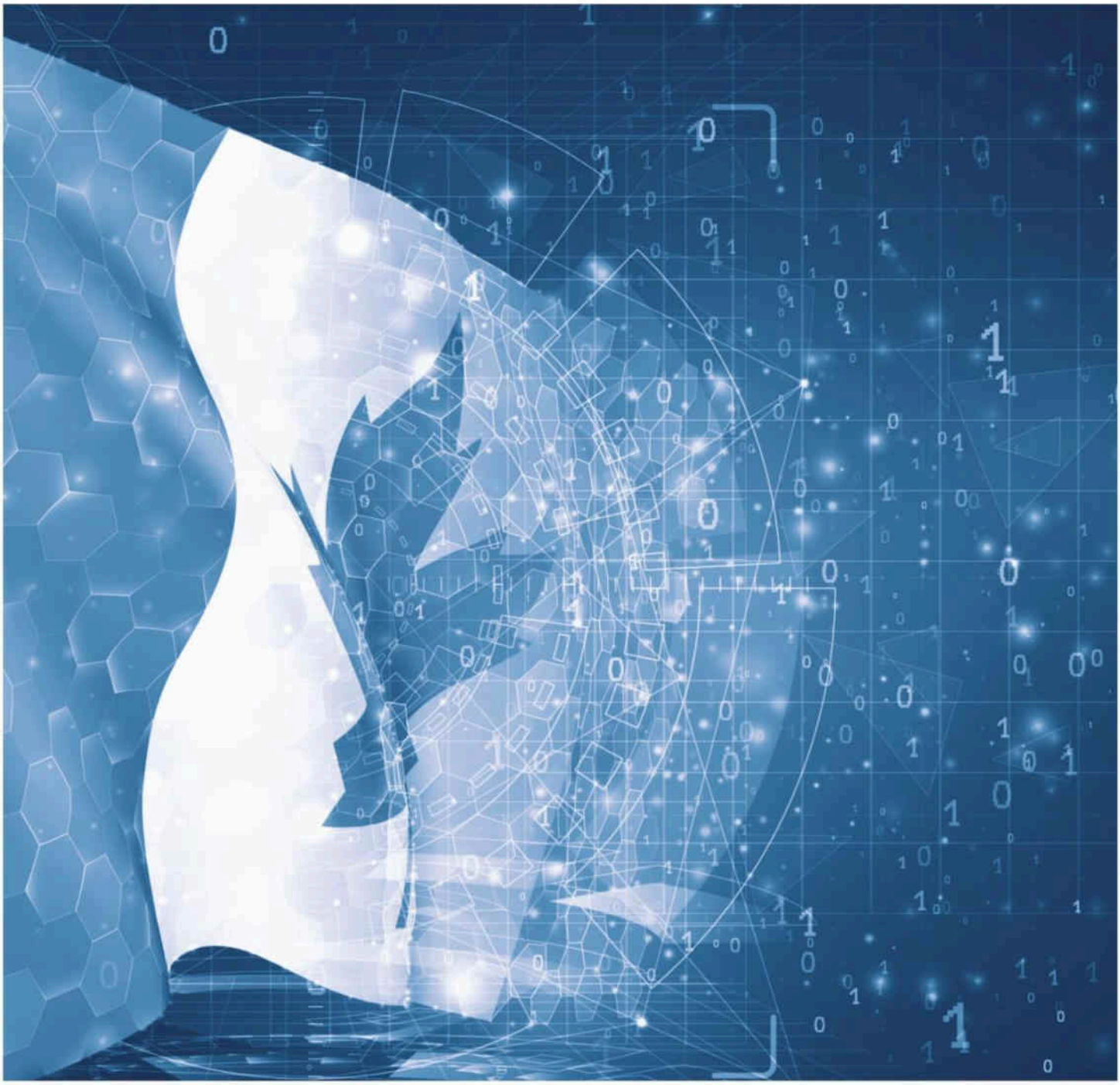
National Security and Intelligence Review Agency | Office de surveillance des activités en matière de sécurité nationale et de renseignement

Canada

NSIRA

2022 // Annual Report



© His Majesty the King in Right of Canada, as represented
by the National Security and Intelligence Review Agency, 2023.
ISSN 2563-5778
Catalogue No. PS106-9E-PDF

September 29, 2023

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 fourth annual report. Consistent with subsection 38(1) of *the National Security and Intelligence Review Agency Act*, the report includes information about our activities in 2022, 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 iv

01 // Introduction 1

1.1 Who we are 1

1.2 Mandate 1

02 // Observations and themes 3

03 // Reviews 6

3.1 Canadian Security Intelligence Service reviews 6

3.2 Communications Security Establishment reviews 14

3.3 Other departments 22

3.4 Multi-departmental reviews 25

3.5 Closed review work 27

3.6 Technology in review 28

3.7 Engagement with reviewees 29

04 // Complaints investigations 33

4.1 Overview 33

4.2 Ongoing initiatives 34

4.3 Investigation report summaries 35

4.4 Statistics on complaints investigations 40

05 // Expanding NSIRA partnerships 41

06 // Conclusion 45

07 // Annexes 46

Annex A: Abbreviations 46

Annex B: Financial overview, staffing, achievements and priorities 48

Annex C: Review findings and recommendations 51

Annex D: Statistics on complaints investigations 81

Endnotes 83

Message from the members

As we reflect on this past year's work, the National Security and Intelligence Review Agency (NSIRA) is proud of what it has accomplished. We pushed past the challenges of the pandemic and pursued our mission with renewed energy and innovation, understanding that we can adapt and even thrive in this new environment. In 2022, our agency focused on building out and refining its processes as we empowered our review and complaints professionals in their work. These efforts enhanced our ability to meet the challenges of our review and investigations mandates, and thereby improve the transparency and accountability of the national security and intelligence activities across the federal government.

In addition to completing a wide array of reviews and investigations, we have stepped back to reflect on our work and activities over the first few years of our mandate. Despite being a relatively new agency, we are now in the position to make broader observations on the themes and trends in our work, and on the community we review. Indeed, as our experience grows, our approaches in our reviews and investigations mature and evolve. We meet our goals of increased efficiency and expertise through a commitment to address the challenges we face, and by seeking out best practices through expanded partnerships with like-minded domestic and international institutions.

During NSIRA's brief history, ministers of the Crown have referred certain matters to us for review, as provided for in the *National Security and Intelligence Review Agency Act*. At the time of writing, we are in the process of such a referral. As this important review progresses, we will ensure that our commitment to independent and professional review is reflected in all our activities.

This report continues themes from previous annual reports by presenting an overview of our work, a discussion on our engagement with reviewees, and an account of the initiatives we undertook to ensure that our products are complete, thorough and professional. It is our belief that as we grow, we bring confidence to the Canadian public with each review and investigation we conduct.

We would like to thank our previous members, Ian Holloway and Faisal Mirza, for their commitment and contribution to advancing the important work of NSIRA during their tenure, and we wish them well in their future endeavours. Finally, we thank the staff of NSIRA's Secretariat for their professionalism and dedication to fulfilling the agency's mandate, and we have no doubt that the year ahead will bring further success for NSIRA.

Marie Deschamps **Marie-Lucie Morin** **Foluke Laosebikan**
Craig Forcese **Matthew Cassar**

Executive summary

1. In 2022, the National Security and Intelligence Review Agency (NSIRA) continued to execute its review and investigations mandates with the goal of improving national security and intelligence accountability and transparency in Canada. This related not only to the activities of the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), but also to other federal departments and agencies engaged in such activities, including:

    - the Department of National Defence (DND) and the Canadian Armed Forces (CAF);
    - the Canada Border Services Agency (CBSA); and
    - all departments and agencies engaging in national security or intelligence activities in the context of NSIRA's yearly reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*.

2. NSIRA has reflected on its work to date and found that a horizontal view of all its findings and recommendations over the past three years reveals the emergence of three major themes: governance; propriety; and information management and sharing. NSIRA observes that there is an interconnected and overlapping aspect to these issues, and as a result believes that improvements to governance could result in broader improvements across all themes.

Reviews

3. The following are highlights of the reviews completed in 2022 along with key outcomes. The number of reviews defined as completed does not include any ongoing reviews, or reviews completed in previous years but that went through or are in the process of going through consultations for their release to the public. Annex C lists all the findings and recommendations associated with reviews completed in 2022, along with the corresponding responses from reviewees, if provided.

4. In addition to the reviews discussed below, NSIRA determined that a number of ongoing reviews would be closed or terminated. These decisions, based on a variety of considerations, allow NSIRA to redirect its efforts and resources towards other important issues.

Canadian Security Intelligence Service

5. In 2022, NSIRA completed the following reviews on CSIS activities:

    - the third annual review of CSIS's threat reduction measures, which provided an overview of all such measures conducted in 2021, and also focused on a subset of these measures to consider the implementation of each measure, how what happened aligned with what was originally proposed, and, relatedly, the role of legal risk; and
    - an annual review of CSIS's activities, which informed, in part, NSIRA's 2022 annual report to the Minister of Public Safety.

Communications Security Establishment

6. In 2022, NSIRA completed two dedicated reviews of CSE, and commenced an annual review of CSE activities:

    - a review of CSE's active and defensive cyber operations (ACO/DCO), which is a continuation of NSIRA's 2021 review of the governance of ACO/DCO by CSE and Global Affairs Canada;
    - a review of a sensitive CSE foreign intelligence collection program, which assisted NSIRA in better informing the Minister of National Defence about CSE's activities; and
    - an annual review of CSE activities similar to that for CSIS, begun for the first time in 2022 and that informed, in part, NSIRA's 2022 annual report to the Minister of National Defence.

Department of National Defence and the Canadian Armed Forces

7. In the course of a review of the Department of National Defence and Canadian Armed Forces (DND/CAF) human source handling activities, NSIRA issued to the Minister of National Defence a report on December 9, 2022, under section 35 of the *National Security and Intelligence Review Agency Act* in relation to a specific operation. Section 35 requires that NSIRA submit to the appropriate Minister a report with respect to any activity that is related to national security or intelligence that, in NSIRA's opinion, may not be in compliance with the law. NSIRA will complete the broader review of DND/CAF's human source handling activities in 2023.

Canada Border Services Agency

8. NSIRA completed its first in-depth review of national security or intelligence activities of the Canada Border Services Agency (CBSA) in 2022: a review of air passenger targeting. This

review examined the CBSA's pre-arrival risk assessment of passengers based on data collected by commercial air carriers. It evaluated whether the CBSA's activities complied with legislative requirements and Canada's non-discrimination obligations.

Multi-departmental reviews

9. NSIRA conducted two mandated multi-departmental reviews in 2022:

    - 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*.

Review work not resulting in a final report

10. During the past year NSIRA determined that certain ongoing review work would be closed or not result in a final report to a Minister. These decisions allow NSIRA to remain nimble and to pivot its work plan. Multiple considerations can lead to the decision to close a review, and doing so allows NSIRA to redirect efforts and resources.

Technology in review

11. In 2022, NSIRA expanded its Technology Directorate to keep pace with the national security and intelligence community's evolving use of digital technologies. The team comprises technical experts and review professionals, who are supported by academic researchers. This expanded team launched NSIRA's first technology-led review, focusing on the lifecycle of warranted CSIS information. In addition to directly supporting NSIRA's reviews, the Technology Directorate also began hosting learning sessions and discussion forums designed to enhance NSIRA employees' knowledge of broader technical issues.

Engagement with reviewees

12. NSIRA continues to address and improve on aspects of its interaction with reviewees during the review process. It saw both improvements and ongoing challenges, and seeks to provide full and transparent assessments in this regard. Updated criteria will be used to evaluate engagement. These criteria are critical for supporting NSIRA's efforts during a review. This approach builds on the agency's previous confidence statements and provides a more consistent and complete assessment on engagement.

13. NSIRA continues to optimize its methods for accessing, receiving and tracking the information required to complete reviews. This involves ongoing discussions and support from reviewees. Limitations and challenges to this process are addressed directly and are communicated publicly where possible.

Complaints investigations

14. As NSIRA marked its third year of existence in 2022 it continued maturing and modernizing the processes for fulfilling its investigations mandate. The jurisdiction assessment phase was standardized, incorporating a verification protocol for the three agencies for which NSIRA has complaints jurisdiction. To speed up the investigative process, investigative interviews are being used more often, taking over from the formal hearings NSIRA previously relied on.

15. The pandemic continued to impact the investigative landscape in the first half of 2022. COVID protocols conflicted with security protocols for investigations, which require in-person meetings. Processes introduced in 2022 are expected to reduce delays in the conduct of investigations on a forward basis.

16. The number of investigation activities last year remained high and included the completion of a referral of a group of 58 complaints by the Canadian Human Rights Commission.

17. Data management and service standards initiatives that were launched are expected to enhance complaint file management in the coming year.

Partnerships

18. During the past year, NSIRA expanded its engagement with valuable partners, both domestically and internationally, and has already reaped the benefits through the exchange of best practices. As a relatively new agency, NSIRA sees such relationships as a priority for its institutional development. NSIRA had the privilege of visiting many international partners as an active participant in the Five Eyes Intelligence Oversight and Review Council, and also engaged other European partners through various forums that bring together like-minded oversight, review and data protection agencies from all over the world.

01 //

Introduction

1.1 Who we are

19. Established in July 2019, the National Security and Intelligence Review Agency (NSIRA) is an independent agency that reports to Parliament. Canadian review bodies before NSIRA did not have the ability to collaborate or share their classified information but were each limited to conducting reviews on a specified department or agency. By contrast, NSIRA has the authority to conduct an integrated review of Government of Canada national security and intelligence activities, and Canada now has one of the world's most extensive systems for independent review of national security.

1.2 Mandate

20. NSIRA has a dual mandate to conduct reviews on and carry out investigations of complaints related to Canada's national security or intelligence activities.

Reviews

21. 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 both the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), as well as the activities of any other federal department or agency that are related to national security or intelligence. Further, NSIRA reviews any national security or intelligence matters that a minister of the Crown refers to NSIRA.[2]

Investigations

22. In addition to its review mandate, NSIRA is responsible for investigating complaints related to national security or intelligence. This duty is outlined in paragraph 8(1)(d) of the NSIRA Act, and involves investigating complaints about:

    - the activities of CSIS or CSE;

- decisions to deny or revoke certain federal government security clearances; and
- ministerial reports under the *Citizenship Act* that recommend denying certain citizenship applications.

23. This mandate also includes investigating national security-related complaints referred to NSIRA by the Civilian Review and Complaints Commission for the RCMP (the RCMP's own complaints mechanism)[3] and the Canadian Human Rights Commission.

02 //

Observations and themes

24. NSIRA has a horizontal, in-depth view of the Canadian national security landscape that allows for an assessment of Canada's complex, interwoven approach to national security. NSIRA annual reports discuss its activities within that framework. This annual report provides an opportunity to reflect on NSIRA's body of work horizontally, and consider what broad trends or themes emerge.

25. NSIRA findings and recommendations touch on many aspects of government activities and operations. Grouping all findings and recommendations according to topics that fall under three broad themes helps simplify a horizontal assessment of trends to date. This categorization and the terminology used may evolve over time.

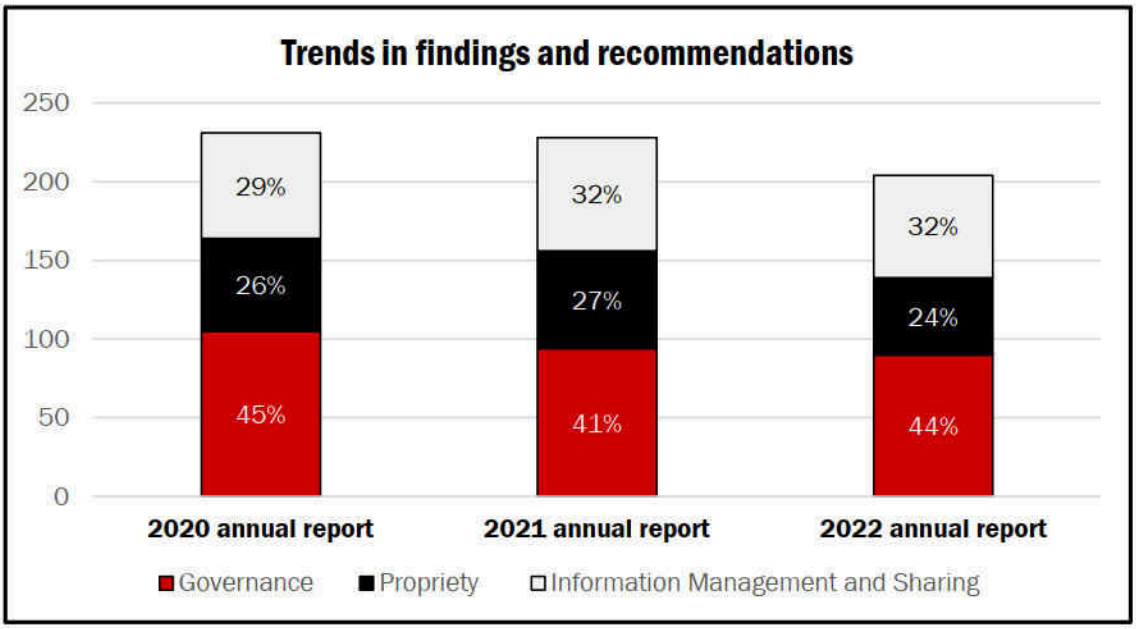
26. The themes that emerge are governance; propriety; and information management and sharing. These themes appear year after year in NSIRA annual reports. The following topics are included in these themes:

Theme	Topics
Governance	• Policies, procedures, framework and other authorities • Internal oversight • Risk management, assessment and practices • Decision-making and accountability, including ministerial accountability and direction • Training, tools and staffing resources
Propriety	• Reasonableness, necessity, efficacy and proportionality • Legal thresholds and advice, compliance and privacy interests
Information management and sharing	• Collection, documentation, tracking, implementing, reporting, monitoring and safeguarding • Information sharing and disclosure • Keeping and providing accurate and up-to-date information, timeliness

27. These themes can be found in every NSIRA annual report, and this year's is no exception. In this year's annual report, the following examples illustrate the three themes:

- governance:
    - the review of disclosures under the *Security of Canada Information Disclosure Act* for 2021 identified that employees did not receive adequate guidance to fulfill their obligations, and recommended improvements to training;
    - the review of a CSE foreign intelligence activity identified several instances where the program's activities were not adequately captured within CSE's applications for certain ministerial authorizations, resulting in recommendations that CSE more effectively inform the Minister of National Defence about aspects of its bilateral relationships with certain partners, the extent of its participation in certain types of activities, and the testing and evaluation of products.
- propriety:
    - in a report issued to the Minister of National Defence under s.35 of the NSIRA Act, NSIRA explained that, in its opinion, certain activities undertaken by the Canadian Armed Forces may not have been in compliance with the law;
    - the review of the threat reduction measures of the Canadian Security Intelligence Service found that this agency did not meet its internal policy requirements regarding the timelines to submit threat reduction measure implementation reports.
- information management and sharing:
    - the Canada Border Services Agency air passenger targeting review noted that this agency does not document its triaging practices that use passenger data in a manner that enables effective verification of whether all triaging decisions comply with statutory and regulatory restrictions.

28. A high-level overview of the past three annual reports shows the number of NSIRA findings and recommendations each year, broken down by theme. Over the three years, governance related findings and recommendations constituted 43% of the overall total. The comparable figures for propriety and information management (IM) and sharing categories were 26% and 31% respectively. The breakdown by year is captured in the following table:



29. The interconnected nature of the problems identified in NSIRA reviews, along with the balance of themes illustrated in the graphic above, reveals a narrative. Indeed, issues rarely stand-alone – governance and IM and sharing issues may, for example, culminate in propriety challenges. The number of findings and recommendations over three years that touch on governance, propriety and IM and sharing matters suggest that these are issues deserving close attention. Employees are expected to succeed in meeting intelligence and national security service missions while adhering to policy and legal requirements. Here, improvements to staff training and development are likely to have the most significant impacts.

03 //

Reviews

30. Details provided on individual reviews are a high-level summary of their content and outcomes. Full versions of each review are available once they have been redacted for public release.

3.1 Canadian Security Intelligence Service reviews

Overview

31. NSIRA has a mandate to review any Canadian Security Intelligence Service (CSIS) activity. The NSIRA Act requires NSIRA to submit an annual report on CSIS activities each year to the Minister of Public Safety and Emergency Preparedness (with these responsibilities now divided into two portfolios, NSIRA currently submits these reports to the Minister of Public Safety). These classified reports include information related to CSIS's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of the exercise of CSIS's powers.

32. In 2022, NSIRA completed one dedicated review of CSIS, and its annual review of CSIS activities, both summarized below. Furthermore, CSIS is implicated in other NSIRA multi-departmental reviews, such as the legally mandated annual reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, the results of which are described in Multi-departmental reviews.

Threat reduction measures review

33. This is NSIRA's third annual review of CSIS threat reduction measures (TRMs), which are measures to reduce threats to the security of Canada, within or outside Canada.[4] Section 12.1 of the *Canadian Security Intelligence Service Act* (CSIS Act) authorizes CSIS to take these measures.

34. NSIRA found that CSIS's activities under its TRM mandate in 2021 were broadly consistent with these activities in preceding years. NSIRA observed that 2018 was an inflection point for CSIS's use of the TRM mandate. In that year, CSIS proposed nearly as many TRMs as were proposed in total in the preceding three years — the first three of the mandate. In the following year,

however, the number dropped slightly, before a more significant reduction in 2020. The number of proposed TRMs in 2021 went up slightly compared with the previous year, as did both approvals and implementations.

35. NSIRA selected three TRMs implemented in 2021 for a more intensive review, assessing the measures for compliance with applicable law, ministerial direction and policy. At the same time, NSIRA considered the implementation of each measure, including the alignment between what was proposed and what occurred, and the role of legal risk assessments for guiding CSIS activity, as well as the documentation of outcomes.

36. For all the measures reviewed, NSIRA found that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the CSIS Act. In addition to general legal compliance, NSIRA found that CSIS sufficiently established a "rational link" between the proposed measure and the identified threat.

37. In one case, NSIRA found that CSIS did not meet its obligations under the 2015 Ministerial Direction for Operations and Accountability and the 2019 Ministerial Direction for Accountability issued by the Minister of Public Safety.

38. The TRM in question involved certain sensitive factors. NSIRA believes that the presence of these factors ought to have factored into the overall risk assessment of the measure. CSIS argued that risks associated with these factors relate primarily to reputational risk to CSIS, which it assessed in this case. Certain risks related to the sensitive factors, however, are not, and in this instance were not, captured by CSIS's reputational risk assessment.

39. Similarly, the legal risk assessment for this TRM did not comply with ministerial direction. NSIRA recommended that legal risk assessments be conducted for TRMs involving these sensitive factors, and further, that CSIS consider and evaluate whether the current process for legal risk assessments complies with applicable ministerial direction.

40. A comparative analysis of the two legal risk assessments provided for the other TRMs under review underscored the practical utility of clear and specific legal direction for CSIS personnel. Clear direction allows investigators to be aware of, and understand, the legal parameters within which CSIS personnel can operate; it also permits reporting after an action is completed to document how implementation stayed within those legal parameters.

41. With respect to documenting outcomes, NSIRA further noted issues with how quickly CSIS produces certain reports after a TRM is implemented. Although NSIRA recognizes that overly burdensome documentation requirements can unduly inhibit CSIS activities, NSIRA

nonetheless believes that the recommendations provided are prudent and reasonable. Relevant information, available in a timely manner, benefits CSIS operations.

Annual review of Canadian Security Intelligence Service activities

42. In 2022, NSIRA completed its annual review of CSIS activities, which aims to identify compliance-related challenges, general trends and emerging issues using CSIS documents in 12 categories (legislatively required and supplementary) from January 1, 2022, to December 31, 2022. Besides contributing to NSIRA's Annual Report to the Minister of Public Safety on CSIS activities, the review may identify areas that merit new NSIRA reviews and may produce a briefing or report with its own observations, findings and recommendations. NSIRA provided its report on CSIS activities in 2021 to the Minister of Public Safety on October 12, 2022, and the Chair subsequently met with the Minister to discuss its contents as well as ongoing issues and challenges related to NSIRA review of CSIS.

Statistics and data

43. 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

44. Section 21 of the CSIS Act authorizes CSIS to make an application 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.[5]

Table 1: Section 21 warrant applications made by the Canadian Security Intelligence Service, 2018 to 2022

	2018	2019	2020	2021	2022
Total section 21 applications	24	24	15	31	28
Total approved warrants	24	23	15	31	28

New warrants	10	9	2	13	6
Replacements	11	12	8	14	14
Supplemental	3	2	5	4	8
Total denied warrants	0	1	0	0	0

Threat reduction measures

45. CSIS is authorized to seek a judicial warrant for a TRM if it believes that certain intrusive measures, outlined in section 21 (1.1) of the CSIS Act, are required to reduce the 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 2: Total number of approved and executed threat reduction measures, 2015 to 2022

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

Canadian Security Intelligence Service targets

46. CSIS is mandated to investigate threats to the security of Canada, including espionage, foreign influenced activities, political, religious or ideologically motivated violence, and subversion.[6] Section 12 of the CSIS Act sets out criteria permitting CSIS 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."[7]

Table 3: Number of Canadian Security Intelligence Service targets, 2018 to 2022

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

Datasets

47. Data analytics is a key investigative tool for CSIS, providing it with the capacity to make connections and identify trends that are not possible through traditional methods of investigation. The *National Security Act, 2017*, which came into force in 2019, gave CSIS new powers, including a legal framework for it to collect, retain and use datasets. The framework authorizes CSIS to collect datasets (divided into Canadian, foreign and publicly available datasets) that have the ability to assist CSIS 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 ministerial accountability. Depending on the type of dataset, CSIS must meet different requirements before it is able to use a dataset.[8]

48. 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 4: Evaluation and retention of publicly available, Canadian and foreign datasets by the Canadian Security Intelligence Service, 2019 to 2022

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

Note: The statistics reported in this table are current as of May 2023. Statistics from previous annual reports have been updated to reflect new data received.

[a] In 2021, CSIS evaluated 4 publicly available datasets and retained 2. Of the other two datasets, it was found that one had been sent late for evaluation so it 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 8 foreign datasets. While no foreign datasets were evaluated in 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

49. The *National Security Act, 2017*, also created a legal justification framework for CSIS's intelligence collection operations. The framework establishes a limited justification for CSIS employees, and persons acting at their direction, to carry out activities that would otherwise constitute offences under Canadian law. CSIS's Justification Framework is modelled on those already in place for Canadian law enforcement.[9] The Justification Framework provides needed clarity to CSIS, and to Canadians, as to what CSIS may lawfully do in the course of its activities. It recognizes that it is in the public interest to ensure that CSIS employees can effectively carry out its 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 and approved by the Intelligence Commissioner. There remain limitations to what activities can be undertaken, and nothing in the Justification Framework permits the commission of an act or omission that would infringe a right or freedom guaranteed by the Charter.

50. According to section 20.1 (2) 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.

Table 5: Authorizations, commissions and directions under the Justification Framework, 2019 to 2022

	2019	2020	2021	2022
Authorizations	83	147	178	172
Commissions by employees	17	39	51	61
Directions to commit	32	84	116	131
Emergency designations	0	0	0	0

Compliance

51. CSIS's internal operational compliance program unit leads and manages overall compliance within CSIS. 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 to provide 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.

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

Table 6: Total number of non-compliance incidents processed by CSIS, 2019 to 2022

	2019	2020	2021	2022
Processed compliance incidents[a]	53	99	85	59
Administrative		53	64	42
Operational[b]	40[c]	19[c]	21	17
Canadian law	—	—	1	2
Charter	—	—	6	5
Warrant conditions	—	—	6	3
CSIS governance	—	—	8	15

[a] Instances of non-compliance processed by CSIS includes instances of non-compliance as well as those instances that were deemed compliant on review by CSIS.

[b] 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, each incident is counted in all 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, which is 17.

[c] 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.

3.2 Communications Security Establishment reviews

Overview

53. NSIRA has the mandate to review any activity conducted by the Communications Security Establishment (CSE). NSIRA must also 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 the exercise of CSE's powers.

54. In 2022, NSIRA completed two dedicated reviews of CSE and commenced an annual review of CSE activities, all summarized below. Furthermore, CSE is implicated in other NSIRA multi-departmental reviews, such as the legally mandated annual reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, the results of which are described in Multi-departmental reviews.

Review of the Communications Security Establishment's active and defensive cyber operations

55. The *Communications Security Establishment Act* (CSE Act) grants CSE the authority to conduct active cyber operations and defensive cyber operations (ACOs and DCOs). CSE ACOs and DCOs have become a tool of Government of Canada foreign and security policy. In 2021, NSIRA reviewed CSE's governance of and the general planning and approval process for ACO and DCO activities.[10] The governance review made several observations about the governance of ACOs and DCOs by CSE — and to a lesser extent, by Global Affairs Canada (GAC). Some of these observations identified gaps that resulted in recommendations. Building on the governance review, the report focused on CSE's ACOs and DCOs themselves:

- the operations;
- the implementation of CSE's governance; and
- the legal framework in the context of specific ACOs and DCOs.

56. NSIRA incorporated GAC, CSIS, the Royal Canadian Mounted Police (RCMP) and DND/CAF into this review, given these organizations' varying degrees of coordination or involvement in these CSE activities. NSIRA also inspected some technical elements of a case study ACO to verify aspects of the operation independently, as well as to deepen NSIRA's understanding of how an ACO works. While NSIRA reviewed all ACOs and DCOs planned or conducted by CSE until mid-

2021, this review focused on a sample of such ACOs or DCOs, each presenting unique characteristics.

57. Overall, NSIRA found that ACOs and DCOs that CSE planned or conducted during the period of review were lawful and noted improvements in GAC's assessments for foreign policy risk and international law. NSIRA further observed that CSE developed and improved its processes for the planning and conduct of ACOs and DCOs in a way that reflected some of NSIRA's observations from the governance review.

58. NSIRA also made findings pertaining to how CSE could improve aspects of ACO and DCO planning, as well as communication to the Minister of National Defence and coordination with other Government of Canada entities. More specifically, NSIRA identified areas of potential risk:

- GAC's capability to independently assess potential risks resulting from CSE ACOs and DCOs;
- the accuracy of information provided, and issues related to delegation, within some of the applications for authorizations for ACOs and DCOs;
- the degree to which CSE engaged with CSIS and the RCMP on ACOs and DCOs, and CSE explanations of how it determined whether the objective of an ACO or DCO could not reasonably be achieved by other means;
- the extent to which CSE described the intelligence collection that may occur alongside or as a result of ACOs or DCOs in applications for ACO and DCO authorizations and in operational documentation; and
- overlap between activities conducted under the ACO and DCO aspects of CSE's mandate, as well as under all four aspects of CSE's mandate.

59. It should be noted that NSIRA faced significant challenges in accessing CSE information on this review. These access challenges had a negative impact on the review. As a result, NSIRA could not be confident in the completeness of information provided by CSE.

Review of a foreign intelligence activity

60. In 2022, NSIRA completed a review of a sensitive CSE foreign intelligence collection program. As part of this review, NSIRA made several findings and observations regarding the activities carried out as part of this program. Notably, NSIRA identified several instances where the

program's activities were not adequately captured within CSE's applications for certain ministerial authorizations. As such, NSIRA recommended that CSE more effectively inform the Minister of National Defence about aspects of its bilateral relationships with certain partners, the extent of its participation in certain types of activities, and the testing and evaluation of products.

61. NSIRA also found several areas where the program lacked adequate governance structures, resulting in improper application of key policy and procedural requirements related to information sharing, confirmation of foreignness, and CSE's mistreatment risk assessment process. NSIRA made recommendations to strengthen these processes, to establish governance structures specific to the program, and to improve other governance structures with broader applicability throughout CSE.

Annual review of Communications Security Establishment activities

62. In 2022, NSIRA launched the annual review of CSE activities, which aimed to identify compliance-related challenges, general trends and emerging issues using CSE documents in 11 categories (legislatively required and supplementary) from January 1, 2022, to December 31, 2022. Besides contributing to NSIRA's Annual Report to the Minister of National Defence on CSE activities, the review may identify areas that merit new NSIRA reviews and may produce a briefing or report with its own observations, findings and recommendations. It is based largely on the structure of the annual review of CSIS activities but has been adapted to CSE. NSIRA's Chair met with the Minister of National Defence on December 15, 2022 to discuss ongoing issues and challenges related to NSIRA reviews of CSE activities.

Statistics and data

63. 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 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

64. Ministerial authorizations are issued to CSE by the Minister of National Defence. Those authorizations support specific foreign intelligence or cybersecurity activities or defensive or active cyber operations conducted by CSE pursuant to those aspects of the CSE 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 7: Ministerial authorizations issued, 2019 to 2022

Type of ministerial authorization	Enabling section of the CSE Act	Issued in 2019	Issued in 2020	Issued in 2021	Issued in 2022
Foreign intelligence	26(1)	3	3	3	3
Cybersecurity – federal and non-federal	27(1) and 27(2)	2	1	2	3
Defensive cyber operations	29(1)	1	1	1	1
Active cyber operations	30(1)	1	1	2	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 2021 and remained in effect in parts of 2022, it is counted solely as a 2021 ministerial authorization.

65. 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 8: Ministerial orders in effect as of 2022

Name of ministerial order	Enabling section of the CSE Act
Designating electronic information and information infrastructures of importance to the Government of Canada	21(1)
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	45 and 44(1)
Designating recipients of Canadian identifying information used, analyzed or retained under a foreign intelligence authorization pursuant to section 45 of the CSE Act	45 and 43
Designating electronic information and infrastructures of Ukraine as Systems of Importance	21(1)
Designating electronic information and infrastructures of Latvia as Systems of Importance	21(1)

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

Foreign intelligence reporting

66. 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 9: Number of foreign intelligence reports issued, 2019 to 2022

CSE foreign intelligence reporting	2019	2020	2021	2022
Number of reports released	N/A	N/A	3,050	3,185
Number of departments/agencies	N/A	>25	28	26
Number of specific clients within departments/agencies	N/A	>2,100	1,627	1,761

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

67. Information relating to a Canadian or a person in Canada (IRTC) is the 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 the acquisition of this information 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.

68. CSE was asked to release statistics or data about the regularity with which IRTC or "Canadian-collected information" is included in CSE's end-product reporting. CSE responded that "this information remains at a classified level. We have determined that the release of this information would be injurious to Canada's international relations, national defence and security. Furthermore, the sharing of this information would provide an additional level of detail on the success of Canadian collection programs, our level of reliance on information from Five-Eye partners to produce intelligence, as well as a level of detail on Five-Eye use and reporting from Canadian collection that has not been previously made public."

Canadian identifying information

69. CSE is prohibited from directing its activities at Canadians or persons in Canada. However, CSE's collection methodologies sometimes result in incidentally acquiring such information. When such incidentally collected information is used in CSE's foreign intelligence reporting, any part potentially identifying 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 10: Number of requests for disclosure of CII, 2021 and 2022

Type of request	2021	2022
Government of Canada requests	741	657
Five Eyes requests	90	62
Non-Five Eyes requests	0	0
Total	831	719

70. In 2022, of the 719 requests received, CSE reported having denied 65 requests. By the end of the year, 51 were still being processed.

71. CSE was asked to release the number of instances where CII is suppressed in CSE foreign intelligence or cyber security reporting. It indicated that "[d]isclosure of the number of instances where [CII] is suppressed in CSE intelligence reporting would be injurious to CSE's capabilities. Such a disclosure would reveal information about CSE's capabilities including their limitations. Thus, this information could be used by hostile security threats to counter CSE's capabilities impeding CSE's ability to protect Canada and its citizens."

Privacy incidents and procedural errors

72. 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 via its Privacy Incidents File[11] and, for privacy incidents that are attributable to a second-party partner or a domestic partner, its Second-party Privacy Incidents File.

Table 11: Number of privacy incidents recorded by CSE, 2021 and 2022

Type of incident	2021	2022
Privacy incidents	96	114
Second-party privacy incidents	33	23

Cyber security and information assurance

73. 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 as being of importance to the Government of Canada.

74. 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, that is, email containing malware;
- unauthorized access to corporate information technology (IT) environments;
- imminent ransomware attacks; and
- zero-day exploits, which involves exploration of critical vulnerabilities in unpatched software.

Table 12: Number of cyber incident cases opened by CSE, 2022

Type of cyber incident	2022
Federal institutions	1,070
Critical infrastructure	1,575
Total	2,645

Defensive and active cyber operations

75. Under section 18 of the CSE Act, CSE is mandated to conduct DCOs 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.

76. Under section 19 of the CSE Act, CSE is mandated to conduct ACOs against foreign individuals, states, organizations or terrorist groups as they relate to international affairs, defence or security.

77. CSE was asked to release the number of DCOs and ACOs approved, and the number carried out, during 2022. CSE responded that it is "not in a position to provide this information for publication by NSIRA, as doing so would be injurious to Canada's international relations, national defence, and national security."

Technical and operational assistance

78. 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).[12]

Table 13: Number of requests for assistance received and actioned by CSE, 2020 to 2022

	2020	2021	2022
Approved	23	32	59
Not approved	1	3	Not applicable
Cancelled	Not available	Not available	1
Denied	Not available	Not available	2
Total received	24	35	62

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. For 2022, CSE was now able to provide the number of requests for assistance approved, denied or cancelled.

3.3 Other departments

Overview

79. In addition to the CSIS and CSE reviews above, NSIRA completed the following reviews of departments and agencies in 2022:

- A review of the Department of National Defence and the Canadian Armed Forces;
- A review of the Canada Border Services Agency; 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.

Department of National Defence and the Canadian Armed Forces

Report issued pursuant to section 35 of the NSIRA Act

80. In the course of a review of the Department of National Defence and the Canadian Armed Forces (DND/CAF) human source handling activities, which was still ongoing at the time of writing, NSIRA issued on December 9, 2022, a report under section 35 of the NSIRA Act to the Minister of National Defence. According to section 35, NSIRA must submit to the appropriate minister a report with respect to any activity that is related to national security or intelligence that, in NSIRA's opinion, may not be in compliance with the law. The Minister of National Defence submitted a copy of this report to the Attorney General of Canada and included her comments indicating that her interpretation of the facts and law differs from NSIRA's. NSIRA stands by its position and is of the view that the Minister's position is based on a narrow interpretation of the facts and the law. NSIRA will complete the larger review of DND/CAF's human source handling activities in 2023. While the section 35 report does not include recommendations, the broader review will examine accountability and oversight of the program, its risk framework, and DND/CAF's discharge of its duty of care with respect to human sources. The review also assesses the lawfulness of the program and its related activities, as well as the sufficiency of its legal and policy foundations. In doing so, the report may include recommendations addressing the observations made in the section 35 report.

Canada Border Services Agency

Air passenger targeting review

81. The Canada Border Services Agency (CBSA) air passenger targeting program uses pre-arrival risk assessments to identify inbound air travellers at higher risk of being inadmissible to Canada or whose entry, or that of their goods, may otherwise contravene the CBSA's program legislation.

82. The first step in these multi-stage assessments is to triage travellers based on the characteristics and travel patterns conveyed to the CBSA by commercial air carriers in Advance

Passenger Information and Passenger Name Record data. This triage may be manual (flight list targeting) or automated (scenario-based targeting). In both methods, the CBSA relies on information and intelligence from a variety of sources to determine which data elements to treat as indicators of risk in relation to particular enforcement issues, including those related to national security. Use of these indicators may lead the CBSA to differentiate among travellers in subsequent stages of targeting or at the border, with impacts on passengers' time, privacy and equal treatment.

83. The review of air passenger targeting was NSIRA's first in-depth assessment of the CBSA's compliance with relevant law. It focused, first, on whether the CBSA complies with restrictions on the use of passenger data established by the *Customs Act* and the *Protection of Passenger Information Regulations*. Next, the review examined whether the CBSA's use of these types of passenger data was discriminatory under the *Canadian Human Rights Act* and the *Canadian Charter of Rights and Freedoms*.

84. NSIRA found that the CBSA's use of both types of passenger data in scenario-based targeting was for a purpose authorized by the *Customs Act*. For flight list targeting, however, the CBSA does not document the reasons underpinning its triage decisions. NSIRA was therefore unable to verify compliance of flight list targeting with the purpose limitations set out in the *Customs Act*. As well, the documentation did not allow NSIRA to verify that the CBSA's use of Passenger Name Record data in either triage method complied with the *Protection of Passenger Information Regulations*, which require that access to retained data be for a purpose related to the identification of persons who have or may have committed a terrorism offence or serious transnational crime.

85. NSIRA also found that the CBSA did not consistently demonstrate an adequate justification for its selection of particular indicators as signals of increased risk. When adequate justification is not present, differentiating among passengers on the basis of prohibited grounds of discrimination (such as age, national or ethnic origin, or sex) creates a risk of discrimination.

86. NSIRA recommended that the CBSA document its triage practices in a manner that demonstrates compliance with the *Customs Act* and, where applicable, the *Protection of Passenger Information Regulations*. It recommended that the CBSA ensure, in an ongoing manner, that its selection of risk indicators be adequately justified based on well-documented information or intelligence. NSIRA further recommended that the CBSA develop more robust and regular oversight of air passenger targeting, including updates to policies, procedures, training and other guidance. NSIRA also recommended that the CBSA begin collecting the data

necessary to identify, analyze and mitigate discrimination-related risks stemming from air passenger targeting.

3.4 Multi-departmental reviews

Review of federal institutions' disclosures of information under the *Security of Canada Information Disclosure Act* in 2021

87. The review of federal institutions' disclosures of information under the *Security of Canada Information Disclosure Act* (SCIDA) in 2021 describes the results of a review of the 2021 disclosures made by federal institutions under this legislation.[13] In 2022, NSIRA focused the review on Global Affairs Canada (GAC)'s proactive disclosures.

88. The SCIDA encourages and facilitates the disclosure of information between federal institutions to protect Canada against activities that undermine or threaten national security, subject to certain conditions. The SCIDA provides a two-part threshold that must be met before an institution can make a disclosure:

    - that the information will contribute to the exercise of the recipient institution's jurisdiction or responsibilities in respect of activities that undermine the security of Canada (paragraph 5(1)(a)); and
    - that the information will not affect any person's privacy interest more than reasonably necessary in the circumstances (paragraph 5(1)(b)).

89. The SCIDA also includes provisions and guiding principles related to the management of disclosures, including accuracy and reliability statements and record keeping obligations.

90. NSIRA identified concerns that demonstrate the need for GAC to improve its training. NSIRA found that there is potential for confusion on whether the SCIDA is the appropriate mechanism for certain disclosures of national security–related information. For some disclosures, GAC did not meet the two-part threshold requirements of the SCIDA before disclosing the information, which was not compliant with the SCIDA. Two disclosures did not contain accuracy and reliability statements, as required under the SCIDA. With respect to record keeping, NSIRA recommended that departments document, at the same time as they are deciding to disclose information under the SCIDA, the information they are relying on to satisfy themselves that the disclosure is authorized under the Act (paragraph 9(1)(e)).

Review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2021

91. This review focused on departmental implementation of directions received through orders in council issued under the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACA). This was NSIRA's third annual statutorily mandated review of the implementation of all directions issued under the ACA. It assessed departments' implementation of the directives received under the ACA and their operationalization of frameworks to address ACA requirements. As such, this review constitutes the first in-depth examination of the ACA within individual departments.

92. This year's review covered the 2021 calendar year and was split into three sections. Section one addressed the statutory obligations of all departments. Sections two and three were an in-depth analysis of how the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC) have implemented the directions under the ACA. NSIRA used case studies, where possible, to examine these departments' implementation of their ACA framework.

93. This was the third consecutive year where no cases were referred to the deputy head level in any department. This is a requirement of the orders in council when officials are unable to determine if the substantial risk can be mitigated. Future reviews will be attuned to the issue of case escalation and departmental processes for decision-making.

94. In the 2019 NSIRA Review of Departmental Frameworks for Avoiding Complicity in Mistreatment by Foreign Entities[14], NSIRA recommended that "the definition of substantial risk should be codified in law or public direction." NSIRA noted that some departments have accounted for this gap by relying on the definition of substantial risk in the 2017 ministerial directions. In light of the pending statutorily mandated review of the *National Security Act, 2017* and the importance of the concept of substantial risk to the ACA regime, NSIRA reiterated its 2019 recommendation that the definition of substantial risk be codified in law.

95. In the review of departmental implementation of ACA in 2020, NSIRA identified the Canada Border Services Agency (CBSA) and Public Safety Canada as not yet having finalized their ACA policies. While the CBSA and Public Safety Canada continue to make advancements, these departments have not fully implemented an ACA framework and supporting policies and procedures.

96. The RCMP has a robust framework in place for the triage and processing of cases pertaining to the ACA. The in-depth analysis portion of this review found that the RCMP does not have a centralized system of documenting assurances and does not regularly monitor and update the assessment of the reliability of assurances. The RCMP has also not developed mechanisms to update country and entity profiles in a timely manner, and the information collected through

the liaison officer during an operation is not centrally documented such that it can inform future assessments.

97. In the analysis of one of the RCMP's Foreign Information Risk Advisory Committee case files, NSIRA found that the RCMP's Assistant Commissioner's rationale for rejecting the risk advisory committee's advice did not adequately address concerns consistent with the provisions of the orders in council. In particular, NSIRA found that the Assistant Commissioner erroneously considered the importance of the potential future strategic relationship with a foreign entity in the assessment of potential risk of mistreatment of the individual.

98. NSIRA found that GAC is now strongly dependent on operational staff and heads of mission for decision-making and accountability under the ACA. This is a marked change from the findings of the 2019 review that found decision-making was done by the Ministerial Direction Compliance Committee at Headquarters.

99. GAC has also not conducted an internal mapping exercise to determine which business lines are most likely to be implicated by the ACA. Considering the low number of cases this year and the size of GAC, and that ACA training is not mandatory for staff, NSIRA has concerns that not all areas involved in information sharing within Global Affairs Canada are being properly informed of their ACA obligations.

100. NSIRA also notes that GAC has no formalized tracking or documentation mechanism for the follow-up of caveats and assurances. This is problematic as mission staff are rotational and may therefore have no knowledge of previous caveats and assurances related to prior information sharing instances.

3.5 Closed review work

101. This past year NSIRA determined that certain ongoing review work would be closed or not result in a final report to a Minister. These decisions allow NSIRA to remain nimble and to pivot its work plan. Considerations such as shifting priorities, resourcing demands, ongoing work taking place within the reviewed department, and deconfliction with partner review agencies can all be factors that lead to a decision to close a review. Such decisions allow NSIRA to redirect its efforts and resources towards other important issues, and thereby maximize the value of its work.

102. For example, a review of the Royal Canadian Mounted Police's (RCMP) Operations Research Branch was closed. A contributing factor in this decision was that the RCMP branch in question ceased to operate. Another example is the decision to cease an ongoing review of how the RCMP handles encryption in the interception of private communications in national security criminal investigations. This review was cancelled to support deconfliction efforts with the

National Security and Intelligence Committee of Parliamentarians (NSICOP), who were conducting a similar review. Finally, a review of the Financial Transactions and Reports Analysis Centre's (FINTRAC) terrorist financing and information sharing regime, which was in its early stages, was cancelled at the same time that NSIRA decided to initiate a review of the Canada Revenue Agency's (CRA) Review and Analysis Division, which delivers the CRA's anti-terrorism mandate.

3.6 Technology in review

Integration of technology in review

103. Digital technologies continue to play a crucial role in the operational activities of Canada's national security and intelligence community as agencies increasingly use new technologies to meet their mandates, propose new avenues for activities, and monitor new threats.

104. It remains essential for an accountability body like NSIRA to keep pace with the use of digital technologies in Canada's national security and intelligence community. By staying apprised of rapidly changing technology ecosystems, NSIRA can ensure that the organizations it reviews are pursuing their mandates lawfully, reasonably and appropriately.

105. NSIRA's Technology Directorate is a team of engineers, computer scientists, technologists and technology review professionals. The mandate of NSIRA's Technology Directorate is to:

- lead the review of Information Technology (IT) systems and capabilities;
- assess a reviewed entity's IT compliance with applicable laws, ministerial direction and policy;
- conduct independent technical investigations;
- recommend IT system and data safeguards to minimize the risk of legal non-compliance;
- produce reports explaining and interpreting technical subjects;
- lead the integration of technology themes into yearly NSIRA review plans;
- leverage external expertise in the understanding and assessment of IT risks; and
- support assigned NSIRA members in the investigation of complaints against CSIS, CSE or the RCMP when technical expertise is required to assess the evidence.

106. In 2022, the Technology Directorate grew from one full-time employee to three and welcomed a cooperative education student and two external researchers. With its increased capacity, the Technology Directorate expanded its analysis of technologies in many NSIRA reviews, started formalizing its research methodology, and began hosting micro-learning sessions and

discussion forums focused on relevant technical issues, including dark patterns, open-source intelligence and encryption.

107. The Technology Directorate also began establishing an academic research network with the goal of supporting NSIRA reviews. To date, contributors to the research network have produced valuable internal memos, reports, and discussion forums, which have enhanced NSIRA's knowledge of a broad set of technical issues.

108. During the last year, the Technology Directorate also launched NSIRA's first technology-led review, which focuses on the lifecycle of CSIS information collected by technical capabilities under a Federal Court warrant. This review presents an opportunity for NSIRA to draw on technical standards and review processes used by its Five Eyes peers and the international review and oversight community. NSIRA has been using this review to develop a risk assessment model and technical inspection plan, expanding NSIRA's broader review toolkit.

Future of technology in review

109. During the next year, NSIRA will continue to hire more full-time employees in the Technology Directorate, support cooperative education and use external researchers to add capacity. Doing so will augment NSIRA's ability to keep pace with the rapidly changing and expanding use of digital technologies in Canada's national security and intelligence ecosystem.

110. Building on the successes of its budding academic research network, the Technology Directorate intends to prioritize unclassified research on a number of topics, including open-source intelligence, advertising technologies and metadata (content versus non-content data).

111. NSIRA's Technology Directorate will also support NSIRA's complaint investigations team to understand where and when technology factors into their processes and pursuits.

3.7 Engagement with reviewees

Improvements and ongoing challenges

112. As discussed in previous annual reports, as a new review body, NSIRA experienced initial challenges in its interactions with departments and agencies being reviewed. These challenges are continually being addressed and NSIRA's relationship with reviewees has matured. While work on this front is not done, reviewees have demonstrated improvements in cooperation and support to the independent review process. The following discussion captures general

commentary on the overall engagement with reviewees that were the focus of the past year's reviews. These overviews cover 2022 and up to the date of writing of this report. Related review-specific commentary or issues, where available, are discussed within each review's overview above.

Canadian Security Intelligence Service

113. After temporary restrictions and adjustments related to COVID-19 were lifted, NSIRA returned to its pre-pandemic level of occupancy within CSIS headquarters for CSIS-related reviews. This includes dedicated workspace and building passes for NSIRA employees reviewing CSIS activities. NSIRA employees have direct access to CSIS databases, and CSIS provides any training necessary, when requested, to navigate and access those systems. Generally, CSIS responds to NSIRA requests for information in a reasonably timely manner. Delays and challenges occur on occasion, but communication between NSIRA and CSIS is constructive in resolving issues.

Communications Security Establishment

114. NSIRA continued to use the space it procured within CSE's headquarters in the Edward Drake Building to conduct review-related business. There was little improvement in 2022 to NSIRA's access requirements at CSE. However, as of 2023, NSIRA is piloting limited direct access to CSE's primary corporate document repository, GCDOCS. Issues remain and NSIRA is not in a position to assess the pilot project's utility. In some instances, CSE has improved its responsiveness to NSIRA information requests in terms of timeliness, although some challenges remain with the quality of responses. NSIRA continues to work diligently with CSE to address these concerns.

Department of National Defence

115. Discussions continue with respect to developing dedicated office space and access to networks. While there has been little advancement on longer-term solutions, DND/CAF has worked with NSIRA to provide access to relevant documents, including sensitive files. DND/CAF has provided good access to facilities and people. Generally, responses to requests for information have been timely; however, a lack of proactiveness in DND/CAF disclosures has required NSIRA to send additional requests to ensure completeness and accuracy of information. Overall, the communication between NSIRA and DND/CAF has been constructive.

Royal Canadian Mounted Police

116. The past year was marked by inconsistencies in the RCMP's responsiveness to NSIRA's requests for information. The RCMP has taken steps to add to its capacity to respond to NSIRA, and this has yielded positive results. NSIRA does not have direct access to information systems but has been granted access to the files relevant to the matters under review. NSIRA has, on multiple occasions, had to send additional requests to ensure the completeness of files provided. In most cases, materials are reviewed on site in the dedicated NSIRA office space that has been provided within RCMP Headquarters. Despite challenges earlier in the year, NSIRA generally had access to people, including RCMP regular members who are experts in the areas under review. Overall, the engagement between NSIRA and the RCMP has seen improvements.

Global Affairs Canada

117. GAC has been responsive to NSIRA's requests, made effort to clarify requests, and facilitated all meetings requested. During the review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2021, GAC provided NSIRA with documents requested within a reasonable time frame. NSIRA did not have direct access to GAC systems, however this did not have an impact on NSIRA's ability to verify information or access sensitive files as GAC was able to transfer all materials requested either by email or through their secure portal.

Canada Border Services Agency

118. The CBSA has provided NSIRA with adequate access to information and people. Some challenges in terms of timeliness were resolved promptly after NSIRA sent notice of a pending advisory letter. These challenges appear to be related to the CBSA's lengthy approval process for the release of documents to NSIRA. NSIRA does not have direct access to CBSA systems, but this has not impeded NSIRA's access to sensitive files. Overall, the CBSA has been responsive to NSIRA requests, ensuring that CBSA employees are available to answer NSIRA's questions.

Refining NSIRA's confidence statements

Assessing responsiveness and verification

119. NSIRA continues to place importance on assessing the overall quality and efficiency of its interactions with reviewees. Previously, NSIRA captured this assessment in a "confidence statement," which provided important additional context to the review, apprising readers of the extent to which NSIRA was able to verify necessary or relevant information, and therefore whether its confidence in the information was impacted. These statements were also informed by aspects such as access to information systems and delays in receiving requested information.

120. NSIRA has further refined and standardized its approach for evaluating the key aspects of its interactions with reviewees and going forward will evaluate the following criteria during each review:
    - timeliness of responses to requests for information;
    - quality of responses to requests for information;
    - access to systems;
    - access to people;
    - access to facilities;
    - professionalism; and
    - proactiveness.

Follow-up on timeliness and advisory letters

121. NSIRA's 2021 public annual report committed to addressing the ongoing struggle for timely responses from reviewees for requested information. During the past year, all delays have been captured by a request for information tracking system. The results inform one of the criteria discussed above. Additionally, NSIRA continues to leverage its three-staged approach to address continued delays by sending advisory letters to senior officials and ultimately respective Ministers should delays persist. This advisory tool was used at five occasions in 2022, three of which were sent to CSE, and two to the RCMP.

122. Advisory letters sent to a reviewee during a review may be appended to the final report for both the appropriate minister's and the public's awareness of such delays. Combined with the updated assessment criteria discussed above, NSIRA works to provide transparency and awareness of both the challenges and successes on interactions with those reviewed.

04 //

Complaints investigations

4.1 Overview

123. In the three years since its establishment, NSIRA has focused on reforming the investigative process for complaints and developing procedures and practices to ensure the conduct of investigations is fair, timely and transparent. NSIRA previously reported on the creation of its Rules of Procedure, on its policy to commit to the publishing of redacted investigation reports, and on the implementation of the use of video technology. In the past year, NSIRA streamlined its jurisdictional assessment phase and its investigative process through the increased use of investigative interviews as the principal means of fact finding. These developments enabled NSIRA to deal with a significant volume of complaints over this reporting period.

124. After receiving a complaint, NSIRA must evaluate whether it is within NSIRA's jurisdiction to investigate based on conditions stated in the *National Security and Intelligence Review Agency Act* (NSIRA Act). For complaints against the Canadian Security Intelligence Service (CSIS) or the Communications Security Establishment (CSE), NSIRA must be satisfied that the complaint against the respondent organization refers to an activity carried out by the organization and that the complaint is not trivial, frivolous or vexatious. For complaints referred from the Civilian Review and Complaints Commission (CRCC) of the Royal Canadian Mounted Police (RCMP), NSIRA must receive and investigate a complaint referred to it under subsection 45.53(4.1) or 45.67(2.1) of the *Royal Canadian Mounted Police Act* if satisfied that the complaint is not trivial, frivolous or vexatious or made in bad faith. For security clearance denials, with impacts upon individuals as set out in the NSIRA Act, NSIRA must receive and investigate the complaint.

125. NSIRA has developed a robust process to review and independently verify respondent organization information, mindful of the interests of the complainant and the security imperatives of the organization.

126. In the past, the Security Intelligence Review Committee routinely dealt with complaints related to CSIS by recourse to formal hearings. While NSIRA retains this statutory power, it has sought to make increasing use of interviews to ascertain the evidence required to fully investigate and consider complaints. Considering the security constraints that limit the disclosure of information to complainants during formal hearings, investigative interviews permit NSIRA access to information in a timely manner and are expected to decrease the length of time to

resolve complaints. This will be important as NSIRA deals with an increased complaint case load owing to its mandate (which includes complaints related to CSIS, CSE, RCMP and security clearances), as well as delays resulting from COVID-19 impacts over the last three years.

4.2 Ongoing initiatives

127. NSIRA has committed to establishing service standards for the investigation of complaints, with the goal of completing 90% of investigations within NSIRA service standards by March 2024. During 2022, NSIRA began developing these service standards, which also aim to encourage prompt and efficient administrative decision-making. The service standards will set internal time limits for certain investigative steps for each type of complaint, under normal circumstances. The service standards will specify the circumstances under which those time limits do not apply. The development of the service standards includes tracking and data collection on whether NSIRA is meeting its own service standards in the investigation of complaints. NSIRA will finalize and publish its service standards in 2023 and is committed to reporting on whether they were met.

128. For the year ahead, NSIRA will continue to improve its website to promote accessibility to the investigation of complaints. More specifically, NSIRA will develop an online password-protected portal through which complainants will be able to submit complaints and receive updates on the status of their file.

129. NSIRA began the last phase of the study on race-based data and the collection of demographic information jointly commissioned with the CRCC. The study is assessing the viability of the collection of identity-based and demographic data as part of the CRCC's ongoing anti-racism initiatives. Improved, more precise and more consistent tracking, collection and measurement of data is necessary to support anti-racism efforts in government. In completing the study, the CRCC and NSIRA will be informed on:

- meaningful and purposeful data collection;
- challenges with the collection of data;
- perspective on how the data collected can be applied to address any potential systemic barriers in NSIRA's investigations process and its anti-racism initiatives; and
- public sentiment of the retention of identity-based data.

Observations on areas for legal reform

130. NSIRA notes that some reforms to its legislation would make it easier to fulfill its investigations mandate. Among these would include an allowance for NSIRA members to have jurisdiction to complete any complaint investigation files they have begun, even if their appointment term expires. Broadened rights of access to individuals and premises of reviewed organizations would enhance verification activities.

4.3 Investigation report summaries

Allegations against CSIS's role in delaying security assessments regarding permanent resident and temporary resident visa applications (07-403-30)

Background

131. The complainants filed a complaint against CSIS alleging that it caused delays in their permanent resident and temporary resident visa applications.

Investigation

132. During NSIRA's investigation, CSIS provided its advice in relation to the complainants' permanent resident applications. In light of this information, NSIRA requested confirmation from the complainants regarding whether they still wished to proceed with their complaint. The complainants clarified that they wanted to either receive monetary compensation or an explanation for the delay that occurred in relation to their file.

Conclusion

133. NSIRA informed the complainants that it does not have the authority to make remedial orders such as requiring CSIS to make monetary compensation to a complainant. However, NSIRA inquired whether CSIS was interested in participating in an informal resolution process to resolve some of or all the issues in the complaint. In the context of NSIRA's informal resolution process, information was provided to the complainants regarding CSIS's involvement in their permanent resident and temporary resident visa applications. NSIRA attempted to communicate with the complainants on several occasions to determine whether they had any questions that would assist in clarifying the circumstances of their complaint.

134. NSIRA determined that reasonable attempts had been made to communicate with the complainants and issued reasons deeming the complaint abandoned as per NSIRA's Rules of Procedure. The complaint investigation file was closed.

Allegations against CSIS, Immigration, Refugees and Citizenship Canada, the Canada Border Services Agency, and Public Safety Canada in relation to their role in processing immigration applications (07-405-1 et al.)

Background

135. Under subsection 45(2) of the *Canadian Human Rights Act*, the Canadian Human Rights Commission (CHRC) referred 58 individual and group complaints to NSIRA. This matter constituted the first time NSIRA had received a section 45 referral from the CHRC.

136. The complainants, Iranian nationals, alleged that the Government of Canada discriminated against them on the basis of national or ethnic origin or race due to the delays in the processing of their temporary or permanent residency visa, or Canadian citizenship.

137. Under section 46 of the *Canadian Human Rights Act*, NSIRA is obliged to conduct an investigation and return a report to the CHRC. It further provides that on NSIRA's report, the CHRC may dismiss the complaint or proceed to deal with the complaint.

138. NSIRA's role in section 45 referrals is confined to scrutinizing the components of a matter that are based on considerations relating to the security of Canada and report findings of its investigation into classified information to the CHRC in an unclassified manner. NSIRA does not possess the authority to exercise the CHRC's statutory discretion to refer the matter to the Canadian Human Rights Tribunal.

Investigation

139. During its investigation, NSIRA considered the evidence given by witnesses and submissions of their counsel during an investigative interview, and the documentation and submissions submitted by the government parties, including classified documents disclosed to NSIRA by CSIS, Immigration, Refugees and Citizenship Canada (IRCC), the Canada Border Services Agency (CBSA) and Public Safety Canada.

140. Importantly, NSIRA heard evidence from the government parties in relation to a particular mandatory indicator developed by the CBSA and used by IRCC officers in deciding referrals for

security screening of Iranian immigration applications. Prior to reforms made by August 2018, one indicator was based entirely on Iranian nationality, coupled only with the age and sex of the applicant. Where an applicant met the criteria, IRCC officers would automatically refer the file to the CBSA and CSIS for security screening. The evidence showed that the government abandoned mandatory indicators in 2018 because of efficacy concerns and because it contributed to delays.

141. NSIRA further noted that IRCC did not keep a record of the particular indicator on which the referral was based. This hindered NSIRA's ability to investigate the other indicators that may have affected the processing of a complainant's immigration application. That being said, NSIRA acknowledged that an indicator tracking code system was being piloted at the time of the investigative interview. This technical solution would allow for the tracking of the IRCC officers' decisions to refer immigration applications for security screening through a coding system identifying the reason for the referral.

Conclusion

142. NSIRA found that:

- the mandatory age and sex indicator used by IRCC in processing immigration applications until May 2018 relied exclusively on nationality, age and sex, which are listed as prohibited grounds of discrimination in section 5 of the *Canadian Human Rights Act*;
- the mandatory age and sex indicator produced a disadvantage (including in terms of delays) to those Iranians who were subjected to security screening and to those whose own files were linked to these applicants;
- at the material times at issue in this matter, the application of that mandatory indicator was not justifiable on national security grounds; and
- the security screening process applicable to citizenship applications in this matter did not produce a disadvantage based on grounds enumerated in the *Canadian Human Rights Act*, as citizenship applications received by IRCC are sent to CSIS for security screening, regardless of the applicant's country of birth.

143. NSIRA submitted its report to the CHRC so that it can assess whether there is a reasonable basis in the evidence for a referral to the Canadian Human Rights Tribunal or whether to dismiss the complaints.

Investigation of a complaint regarding the revocation of a security clearance by the Chief of the Defence Staff (1170-17-7)

Background

144. The complainant was a regular force soldier who held a Top-Secret security clearance. The results of the complainant's polygraph examination, although not exclusively relied on, were the primary influence in the security assessments of the complainant prepared by CSIS and the DND Departmental Security Officer. As a result of those assessments, the Chief of the Defence Staff (CDS) revoked the complainant's security clearance. The complainant filed a complaint with NSIRA against the CDS over the revocation of the security clearance.

Investigation

145. During the Investigation, NSIRA heard from government witnesses from DND and CSIS about the polygraph examination, the investigation into the complainant, and the process leading to the revocation of the complainant's security clearance. In addition to the oral evidence, the government parties filed documents and made submissions. NSIRA also considered the oral evidence and written submissions provided by the complainant.

146. NSIRA reviewed all of the evidence it received to determine whether there were reasonable grounds for the CDS to revoke the complainant's security clearance and to ensure the accuracy of the information the CDS used to reach the decision to revoke.

147. NSIRA found several deficiencies in the way the complainant's polygraph was handled, reported and disseminated. In addition, NSIRA found that exculpatory facts were not contextualized nor placed before the CDS prior to the decision to revoke.

Conclusion

148. NSIRA found that the information the CDS relied on to make the decision to revoke was not accurate. As a result, the decision to revoke the clearance was not reasonable.

149. NSIRA recommended that CSIS apologize to the complainant for the manner in which the polygraph was handled, reported and disseminated and that the CDS revisit the decision to revoke the complainant's security clearance.

Review of the Royal Canadian Mounted Police's report regarding a public complaint (07-407-3)

Background

150. The complainant filed a complaint with the CRCC related to the conduct of members of the RCMP. The complainant alleged that the RCMP carried out an unjustified and arbitrary arrest of their minor son, conducted a zealous and abusive search of the family home, and publicized the arrest.

151. In addition, the complainant alleged that the RCMP disclosed information to U.S. authorities, stated that the complainant's son's arrest form would be forgotten and destroyed, and violated the son's safety and that of his family, their constitutional rights and their whistleblower rights.

152. The RCMP concluded, in a report sent to the complainant pursuant to section 45.64 of the *Royal Canadian Mounted Police Act* (RCMP Act), that the members had acted appropriately and consequently did not support any of the complainant's allegations.

153. The complainant referred their complaint to the CRCC for review as they were not satisfied with the RCMP's findings. The CRCC referred the complaint to NSIRA pursuant to subsection 45.53(4.1) of the RCMP Act.

Investigation

154. NSIRA determined that it had jurisdiction to review the request for review of the RCMP's report under section 19 of the NSIRA Act.

155. NSIRA's investigation included a review of:

- the complaint;
- the complainant's request for review filed with the CRCC;
- the RCMP investigation file related to the complaint, including documents provided by the complainant during the investigation; and
- the RCMP's operational file related to the complaint, including numerous audio and video recordings, as well as relevant policies and legislation.

Conclusion

156. NSIRA found that the RCMP's conclusions in its report were reasonable.

157. Notwithstanding the foregoing, NSIRA pointed out to the RCMP the importance of the decision-maker and signatory of an RCMP report having no prior involvement with the file that is the

subject of the complaint, in addition to the importance of complete and contemporaneous notetaking.

4.4 Statistics on complaints investigations

158. Investigation activity continued at significant levels in 2022 (see Annex D). One noteworthy difference in activity from 2021 to 2022 was the significant decline in the number of active investigations: from 81 in 2021 to 19 in this reporting period. This decrease is largely attributed to a referral of close to 60 related files from the CHRC, which were dealt with during this reporting period.

159. Under section 16 of the NSIRA Act, any person may make a complaint to NSIRA with respect to any activity carried out by CSIS; section 17 covers complaints related to CSE activities. However, for NSIRA to be able to accept a complaint, the complainant to CSIS must first send a letter of complaint to the Director of CSIS; for CSE complaints, a letter must first be sent to the CSE Chief. NSIRA will investigate the complaint if the complainant has not received a response within a period of time that NSIRA considers reasonable or if the complainant is dissatisfied with the response given. In that regard, NSIRA observed that in 2022, 53% of complainants did not receive a letter from CSIS in response to their letter of complaint to the Director of CSIS.

160. There is a need to increase awareness and understanding on the part of members of the public and complainants on NSIRA's investigative mandate and process. For example, NSIRA members do not have the ability to make remedial orders, such as compensation, or to order a government department to pay damages to complainants. NSIRA continues to make improvements to its public website to raise this awareness and better inform the public and complainants on the investigations mandate and investigative procedures it follows.

05 //

Expanding NSIRA partnerships

161. NSIRA believes that establishing a community of practice in the business of independent review and oversight is essential and is actively contributing to this effort. During the past year, it resumed and expanded its engagement with valuable partners, both domestically and internationally, and has already reaped the benefits of these efforts.

International partnerships

162. NSIRA has identified international relationships with counterparts as a priority for its institutional development. During the past year, NSIRA benefited from excellent free-flowing and extensive interactions with its closest international partners. A better understanding of the parameters of the review and oversight activities of NSIRA's international counterparts, and sharing best practices, are vital to the agency's growth.

Five Eyes Intelligence Oversight and Review Council

163. Since its inception, NSIRA has been an active participant in the Five Eyes Intelligence Oversight and Review Council. The council comprises agencies with an oversight and review mandate concerning the national security activities in their respective countries (Canada, Australia, New Zealand, the United Kingdom and the United States). NSIRA participates alongside the Office of the Intelligence Commissioner as Canada's delegation to the council. The group meets annually, and NSIRA participated in the Five Eyes Intelligence Oversight and Review Council conference in Washington D.C. in 2022. NSIRA has the distinct pleasure of hosting council partners in Ottawa in fall 2023.

164. NSIRA also frequently engages bilaterally with council partners at the working level. These exchanges allow NSIRA to better understand critical issues impacting its work, compare challenges and best practices in review and oversight methodology, and discuss views on subjects of mutual interest and concern. For instance, learning about council partners' information access rights, and the legal framework enabling such access, has helped to contextualize some of NSIRA's own access challenges.

165. NSIRA met with one of its council partners, the Investigatory Powers Commissioner's Office in London, U.K. The Commissioner's office has a broad mandate of activities that includes, among others, approving warrants authorized by the Secretary of State and the independent oversight of the use of the powers by the U.K.'s security and intelligence community. The multi-day meetings provided an opportunity to better understand each other's respective organizations, exchange ideas and share best practices. NSIRA met with a number of departments with whom the Commissioner's office engages and shadowed a day-long inspection carried out by the Commissioner's office. Of particular interest was the Commissioner's office's approach for following up on the implementation of recommendations it provides and its insights on the production of annual reports. Support for this important partnership continues, and NSIRA has further engaged with Commissioner's office staff to cement this strong relationship.

166. NSIRA was also able to complete working-level visits to the office of Australia's Inspector-General of Intelligence and Security and to offices of some members of the U.S. inspector general community in Washington.

Additional European engagement

167. NSIRA also participated in the International Intelligence Oversight Forum, which brings together oversight, review and data protection agencies from all over the world. The event was productive and NSIRA had the additional benefit of constructive bilateral exchanges with participating institutions.

168. As part of its efforts to build strong relationships with continental European counterparts in like-minded jurisdictions with strong accountability mechanisms, NSIRA visited the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services, the Danish Intelligence Oversight Board, the Netherlands' Review Committee on the Intelligence and Security Services, and the Swiss Independent Oversight Authority for Intelligence Activities.

169. Each of these highly productive visits allowed NSIRA to learn from these partners and make its work more visible within this review community.

Stronger domestic coordination

170. NSIRA continued to invest in strengthening relationships with key domestic partners — the National Security and Intelligence Committee of Parliamentarians (NSICOP), the Civilian Review and Complaints Commission for the RCMP and the Office of the Intelligence Commissioner, as well as the various agents of Parliament who play a key role in government accountability.

171. NSIRA and NSICOP have complementary roles in enhancing accountability for federal national security and intelligence activities and are required by law to cooperate in the fulfillment of their respective mandates. Regular cooperation meetings are held at various levels and the two agencies continue to refine ways to cooperate and coordinate. NSIRA and NSICOP have supported each other's work by communicating regularly on review plans to avoid duplication and to make adjustments where required. These coordination efforts contributed to NSIRA's decision to cease work on an RCMP encryption review. NSIRA has also provided, after ministerial consultation, many of its final reports to NSICOP. For its part, NSICOP has provided NSIRA with its classified reports and background briefings. These exchanges have allowed both organizations to refine their review topics and methodologies. NSICOP's and NSIRA's legal teams have also engaged productively, with a view to working through common access challenges, among other things. These frequent and in-depth exchanges serve as an important foundation for a cohesive and robust national security and intelligence review apparatus, and NSIRA and NSICOP enjoy a level of cooperation that is among the strongest of their international counterparts.

172. As discussed under Ongoing initiatives, NSIRA and the Civilian Review and Complaints Commission for the RCMP have jointly commissioned a study on race-based data and the collection of demographic information. This study will inform each organization's approach to developing and implementing an identity-based data strategy in the context of its complaints investigations. The study is currently in its last phase and is expected to be completed in fiscal year 2023–2024.

173. In 2022, the NSIRA Secretariat joined a network of legal professionals from across the various agents of Parliament. As a separate agency and separate employer mandated with supporting independent oversight, NSIRA's Secretariat benefits from collaborating with this community of practice through discussions on legal issues of common interest, professional development and knowledge transfer initiatives.

Emerging cooperation in technology

174. Building partnerships allows NSIRA's growing Technology Directorate to gather diverse perspectives, collaborate on common goals, refine methodologies, and build on established best practices. In 2022, the team focused on building relationships with peers who share mandates on technical topics, such as privacy-enhancing technologies, automated decision-making and service design. Within Canada, this included collaboration with the Office of the Privacy Commissioner's Technology Analysis Directorate, the artificial intelligence team at the

Treasury Board Secretariat's Office of the Chief Information Officer, and the Canadian Digital Service.

175. International and academic collaborations offered access to rich technical knowledge and expertise of other review and oversight bodies. Knowledge management, talent retention and evolving technical capabilities became the focal point of regular engagement with teams at the Investigatory Powers Commissioner's Office, Australia's Inspector-General of Intelligence and Security, and the Norwegian Parliamentary Oversight Committee on Intelligence and Security Services. Finally, 2022 gave rise to NSIRA's external research program aimed at informing and supporting reviews already in progress with relevant and timely technical expertise. Building on the past year's efforts, the Technology Directorate intends to continue developing domestic and international partnerships, including expanding its network with academics, civil society and commercial leaders to ensure key technological issues factor into its approaches.

06 //

Conclusion

176. As NSIRA fulfills its role within Canada's security and intelligence landscape, it is continually motivated by the vital importance of its mandate. This is expressed through each review and complaint investigation completed. In executing its mission in 2022, NSIRA continued to build best practices across the agency. This ongoing growth and evolution position it well to take on new challenges.

177. As the agency's experience grows so too does its knowledge, and it is confident in its ability to be a leading voice in the review and investigations discourse. Partnerships and engagement with reviewees are maturing, and NSIRA is already reaping the benefits of significant effort on both fronts. Applying lessons learned from these partnerships allows NSIRA to iterate and improve its processes and approaches. While there is there is still much work ahead, the results are encouraging.

178. As NSIRA's members consider the agency's accomplishments this past year, they are proud of the diligence and enthusiasm that Secretariat staff have demonstrated. NSIRA has risen to the challenge of changing circumstances and growth and have done so with an outstanding professionalism. The agency looks forward to the year ahead as it carries on with its important work.

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
Cyber Centre	Canadian Centre for Cyber Security
CDS	Chief of the Defence Staff
CHRC	Canadian Human Rights Commission
CII	Canadian-identifying information
CRA	Canada Revenue Agency
CRCC	Civilian Review and Complaints Commission for the RCMP
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DCO	defensive cyber operations
DLS	Directorate of Legal Services
DND	Department of National Defence
DOJ	Department of Justice
FINTRAC	Financial Transactions and Reports Analysis Centre
FIRAC	Foreign Information Risk Advisory Committee
GAC	Global Affairs Canada
IRCC	Immigration, Refugees and Citizenship Canada

IRTC	Information relating to a Canadian or a person in Canada
IT	Information technology
JPAF	Joint Planning and Authorities Framework
MA	Ministerial Authorization
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
NSLAG	National Security Litigation and Advisory Group (Justice)
PS	Public Safety Canada
RCMP	Royal Canadian Mounted Police
SCIDA	*Security of Canada Information Disclosure Act*
SIGINT	Signals intelligence
TRM	Threat reduction measure

Annex B: Financial overview, staffing, achievements and priorities

Financial overview

179. The NSIRA Secretariat is organized according to two main business lines: Mandate Management and Internal Services. The table below presents a comparison of spending between 2021 and 2022 for each of these two business lines.

(In dollars)	Expenditures (2022)	Expenditures (2021)
Mandate Management	7,679,950	7,523,552
Internal Services	11,033,465	8,926,178
Total	**18,713,415**	**16,449,730**

180. In the 2022 calendar year, the Secretariat spent $18.7 million, a $2.3 million (14%) increase from the $16.4 million spent in 2021. This spending increase is mainly attributed to the ramping up of a large infrastructure project and an increased use of external services for corporate activities.

Staffing

181. As of June 30, 2023, NSIRA Secretariat staff complement stood at 76. In an attempt to address hiring and retention challenges, the Secretariat implemented several initiatives including the introduction of an internal development program for its mandate management sector employees. The Program aims at promoting existing employees once they acquire the level of knowledge and competencies required to be promoted. The program is individualized, informed by regular review of progress in the achievement of core knowledge and competencies expectations. The Secretariat has also launched a program to hire recent Ph D. graduates in fields of expertise that are of interests to NSIRA's mandate.

182. The Secretariat also continues to use modern and flexible staffing strategies, procedures and practices. It has adapted its operations and activities to allow, to the extent possible, a flexible hybrid work model.

183. Clearer articulation of its core competency profiles, operational methodologies and practices also enabled a more effective integration and onboarding of employees into the organization.

184. Having hired a dedicated employee responsible for the implementation of an employee wellness agenda combined with an active Mental Health and Wellness Committee, several initiatives have been delivered in an aim to foster workplace well-being and increased interactions between employees.

Progress on foundational initiatives

Accessibility, employment equity, diversity, and inclusion

185. Informed by its three-year action plan and its commitments to the Clerk of the Privy Council, the Secretariat's internal committee responsible for accessibility, employment equity, diversity and inclusion invited guests and led discussions aimed at increasing awareness, celebrating the Secretariat's diverse workforce, and identifying barriers and solutions with respect to these themes.

186. NSIRA also took concrete steps as part of its mandated activities to include, among other things, a Gender-based Analysis Plus lens into the design and implementation of its policies and programs. As a result, NSIRA's renewed forward-looking review plan is informed by considerations related to anti-racism, equity and inclusion. These considerations apply to the process of selecting reviews to undertake, as well as to the analysis that takes place within individual reviews. NSIRA reviews routinely consider the potential for national security or intelligence activities to result in disparate outcomes for various communities and will continue to do so in the year ahead.

187. In 2022, NSIRA also continued to work with another review body to develop strategies for the collection, analysis and use of identity-based data. The goal of the exercise is to rely on public consultations to determine how the public perceives the collection, analysis and use of identity-based data in relation to mandate.

188. Finally, the Secretariat also developed and posted its inaugural accessibility plan on NSIRA's external website. The plan outlines the steps that will be taken over the next three years to increase physical and information accessibility, both for employees within the organization as well as for Canadians more generally.

Facilities projects, technology and security

189. The Secretariat is in the process of retrofitting additional workspace to enable it to accommodate all its employees within the confines of one building. The construction phase is

expected to be completed late in 2023. Over the course of 2022, the Secretariat worked closely with lead security agencies to ensure the fit-up meets best practices and established standards.

Transparency and privacy

190. The Secretariat continues to promote transparency by dedicating resources to redact, declassify and release previous reports from the Security Intelligence Review Committee, in addition to proactively releasing NSIRA's reviews. In 2022, a major upgrade to NSIRA's external website was initiated with the goal of increasing access to information including access to redacted review reports and recommendations. It is expected that the website will be released in 2023.

191. From a privacy perspective, the NSIRA Secretariat continued to make progress further to the privacy impact assessment exercise conducted in fiscal year 2021-2022 in relation to review activities and internal services. It also initiated a privacy impact assessment for the investigations function. This work is expected to be completed in fiscal year 2023-2024.

192. Considering the importance of privacy as part of its activities, NSIRA took concrete steps to implement best practices to protect the privacy of individuals as part of complaints investigations and as part of the conduct of reviews.

Annex C: Review findings and recommendations

This annex lists the full findings and recommendations for the National Security and Intelligence Review Agency (NSIRA) reviews completed in 2022, as well as reviewees' management responses to NSIRA's recommendations, to the fullest extent possible at the time of publication. NSIRA will update such information from all reviews when they are published on its website.

Canadian Security Intelligence Service review

Threat Reduction Measures Annual Review

NSIRA's findings

1. NSIRA finds that the Canadian Security Intelligence Service's (CSIS's) use of its TRM mandate in 2021 was broadly consistent with its use in preceding years.

2. For all the cases reviewed, NSIRA finds that CSIS met its obligations under the law, specifically the *Canadian Charter of Rights and Freedoms* and sections 12.1 and 12.2 of the CSIS Act.

3. For all the cases reviewed, NSIRA finds that CSIS sufficiently established a "rational link" between the proposed measure and the identified threat.

4. For Case 1 and Case 2, NSIRA finds that CSIS met its obligations under the 2015 Ministerial Direction for Operations and Accountability and the 2019 Ministerial Direction for Accountability issued by the Minister of Public Safety.

5. For Case 3, NSIRA finds that CSIS did not meet its obligations under the 2015 Ministerial Direction for Operations and Accountability and the 2019 Ministerial Direction for Accountability issued by the Minister of Public Safety.

6. With respect to legal risk assessments, NSIRA finds that greater specificity regarding legal risks, and direction as to how said risks could be mitigated and/or avoided, resulted in more detailed outcome reporting vis-à-vis legal compliance.

7. For Case 2 and Case 3, NSIRA finds that CSIS did not meet its obligations with respect to one requirement of its Conduct of Operations, Section 12.1 Threat Reduction Measures, Version 4. CSIS did not meet its internal policy requirements regarding the timelines to submit TRM implementation reports.

8. For Case 3, NSIRA finds that the Intended Outcome Report was not completed in a timely manner.

9. NSIRA finds that current policy for the completion of Strategic Impact Reports may inhibit the timely production of important information.

NSIRA's recommendations

Recommendation
Recommendation 1: NSIRA recommends that formal legal risk assessments be conducted for TRMs involving [*sensitive factors*].
Recommendation 2: NSIRA recommends that CSIS consider and evaluate whether legal risk assessments under TRM Modernization comply with applicable ministerial direction.
Recommendation 3: NSIRA recommends that CSIS work with the Department of Justice to ensure that legal risk assessments include clear and specific direction regarding possible legal risks and how they can be avoided/mitigated during implementation of the TRM.
Recommendation 4: NSIRA recommends that Implementation Reports specify how the legal risks identified in the legal risk assessment were avoided/mitigated during implementation of the TRM.
Recommendation 5: NSIRA recommends that CSIS specify in its *Conduct of Operations, Section 12.1 Threat Reduction Measures* when the Intended Outcome Report is required, as it does for the Strategic Impact Report.
Recommendation 6: NSIRA recommends that CSIS integrate in policy a requirement that the Strategic Impact Report be completed at the expiry of the TRM authority.

Communications Security Establishment reviews

Review of the Communications Security Establishment's Governance of Active and Defensive Cyber Operations — Part 2

NSIRA's findings

1. NSIRA finds that the Global Affairs Canada Foreign Policy Risk Assessment process, as well as the related international legal assessment, improved since the Governance Review, for Communications Security Establishment (CSE) active cyber operations (ACOs) and defensive cyber operations (DCOs).

2. NSIRA finds that Global Affairs Canada does not have capability to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.

3. NSIRA finds that CSE and the Department of Justice demonstrated a thorough understanding of section 32 of the CSE Act. However, CSE does not appropriately consult with the Department of Justice at the [*specific step*][15] stage to ensure that the assessment of legal compliance remains valid.

4. NSIRA finds that CSE's applications for authorizations issued under subsections 29(1) and 30(1) of the CSE Act for [*description*] activities did not include all the available information relevant to a meaningful assessment of the requirements in subsections 34(1) and (4) of the CSE Act.

5. NSIRA finds that there is potential for overlap between CSE and CSIS activities in the context of capabilities used by CSE to conduct its ACOs and DCOs. However, CSE did not consistently consult with CSIS about CSE's cyber operations.

6. NSIRA finds that despite close collaboration with Global Affairs Canada, and the Department of National Defence and Canadian Armed Forces on ACOs and DCOs, CSE did not demonstrate consistent engagement with CSIS or the Royal Canadian Mounted Police (RCMP) to determine whether the objective of an ACO or DCO could not reasonably be achieved by other means.

7. NSIRA finds that the Chief's applications for active and defensive cyber operations activities for the period of review did not accurately describe the relationship between a cyber operation, and intelligence collection.

8. NSIRA finds that, in its [*a specific document*], CSE did not always provide clarity pertaining to foreign intelligence missions.

9. NSIRA finds that CSE's ACOs and DCOs that were planned or conducted prior to July 30, 2021, including the case studies analyzed in this report, were lawful.

10. NSIRA finds that there is significant overlap between activities conducted under the ACO and DCO aspects of CSE's mandate, as well as between all four aspects of CSE's mandate.

NSIRA's recommendations, and CSE response

Recommendation	CSE and GAC Response (June 21st , 2023)
Recommendation 1: NSIRA recommends that Global Affairs Canada develop or otherwise leverage capability to enable it to independently assess potential risks resulting from the techniques used in CSE ACOs and DCOs.	**Disagree**. CSE and GAC disagree with this recommendation. In accordance with the CSE-GAC Governance Framework, GAC assesses CSE cyber operations for foreign policy risks and compliance with international law. CSE's internal risk assessment process assesses the cyber operation for technical risks based on the techniques used. Just as CSE relies upon GAC to provide expertise in foreign policy and international law, GAC relies upon CSE to provide expertise on technologies and techniques at the forefront of development. Accurate assessment of all risks from a cyber operation relies on the continuation of open and honest dialogue and trust between GAC and CSE. As such, CSE will continue to share information with GAC on techniques, whenever their use may have an impact on GAC's foreign policy risk assessment.
Recommendation 2: NSIRA recommends that the Department Justice be fully consulted at all stages of an ACO or DCO, particularly prior to operational execution.	**Agree in principle.** CSE agrees with this recommendation in principle. CSE believes that the advice and guidance provided by the Department of Justice (DOJ) representatives embedded in CSE's Directorate of Legal Services (DLS) is integral to CSE's success. CSE consults with DLS at all relevant stages of a cyber operation. As a matter of practice, CSE consults DLS throughout the Joint Planning and Authorities Framework (JPAF) process and at a key stage, and more consultation is conducted when an activity is new or novel. Internal tools developed by DLS are used to ensure that activities do not contravene the prohibitions set out in the CSE Act and assist analysts in identifying when a higher risk necessitates further legal review. Additionally,

Recommendation	CSE and GAC Response (June 21st , 2023)
	CSE's internal operational policy team is consulted on all key stages.
Recommendation 3: NSIRA recommends that CSE abandon the practice of generic ACO and DCO applications to the Minister of National Defence, and instead submit individual applications.	**Disagree.** CSE and GAC disagree with this recommendation. When submitting an application for these particular ACO and DCO Ministerial Authorizations (MAs), CSE and GAC always ensure that the Minister of National Defence and the Minister of foreign Affairs are provided with a sufficient amount of information to make an informed decision as to whether CSE's proposed activities are reasonable and proportionate against a specific set of objectives. To that end, these particular ACO and DCO MAs are structured around key objectives in countering a number of well-defined threats globally. In that sense, they are not "generic", but their scope is broad enough to give CSE the flexibility to act against a wide range of targets, when the identity of threat actor or the location and context is unknown at the time of application. For any operations assessed as falling under the authority of these MAs, the current governance framework allows for appropriate risk management of operations. CSE provides GAC with detailed mission plans for each operation, which allows for a proper assessment of foreign policy risks associated with CSE's cyber operations. Following Recommendation no. 1 from the Governance review (FCO 1), CSE and GAC increased the amount of information included in the 2021 application for this MA. The level of detail was improved further in the 2022 application. Moreover, CSE and GAC work collaboratively on any new MAs to both ensure that relevant foreign policy objectives are reflected and that authorized operations are sufficiently scoped. Whenever an activity does not fit within

Recommendation	CSE and GAC Response (June 21st, 2023)
	the category covered by these MAs, CSE will submit a new application specific to that circumstance.
Recommendation 4: NSIRA recommends that CSE always engage with CSIS, the RCMP, and any other federal departments or agencies as to whether those departments are in a position to reasonably achieve the objective of a cyber operation.	**Agree.** CSE agrees with this recommendation. CSE values the importance of consulting with all relevant Government of Canada stakeholders. During the planning of operations, CSE has and will continue to strengthen its collaborative relationships with its partners, including engaging with CSIS, RCMP, and other relevant federal departments or agencies whose mandates may intersect with a planned ACO or DCO.
Recommendation 5: NSIRA recommends that the Chief's applications for active and defensive cyber operations inform the Minister of National Defence that acquisition of information under a valid foreign intelligence, cybersecurity, or emergency authorization, [*description*].	**Agree.** CSE and GAC agree with this recommendation. This recommendation has already been addressed in the applications for the 2022-23 ACO and DCO Ministerial Authorizations.
Recommendation 6: NSIRA recommends that documentation prepared as part of the CSE's cyber operations framework provide clear links to all known applicable foreign intelligence (or cybersecurity) missions.	**Agree.** CSE agrees with this recommendation. Since the period under review, and partially stemming from NSIRA recommendations issued in the Governance review (FCO 1), CSE has implemented this change into its cyber operations framework. Under the current framework, the documentation now includes links to s.16 or s.17 operations that are directly relevant to a s.18 or s.19 cyber operation.
Recommendation 7: NSIRA recommends that CSE continue to refine, and to define, the distinctions between activities conducted under different aspects of its mandate, particularly between ACO and DCO activities, but also with regard to foreign intelligence and cybersecurity activities.	**Agree in principle.** CSE agrees with this recommendation in principle. CSE agrees with the principle of understanding the nuances of its mandate. The CSE Act (ss.15-20) expressly distinguishes between the five aspects of the mandate. Operations are planned with an understanding of the scope and boundaries of the authorizing aspect of the mandate. CSE works closely with the Directorate of Legal Services (DLS) and its Operational Policy team to ensure that

Recommendation	CSE and GAC Response (June 21st , 2023)
	operations are planned and conducted under the appropriate authorities. In the body of its report, NSIRA acknowledges both the clarity of the Act and of CSE's ability to explain why an operation should be authorized under a particular aspect of the mandate. CSE's policies and procedures governing the planning and conduct of operations rely on the distinction between aspects of the mandate. CSE's Mission Policy Suite addresses each aspect of the mandate and provides a distinction between ACOs and DCOs. The cyber operations framework provides for planning documentation that sets out why the objectives and nature of the planned operation align with the authorities of an ACO versus a DCO, notwithstanding the techniques being applied. Finally, CSE is in the process of launching updated legal and policy training to its operational staff.

Foreign intelligence review

NSIRA's findings

1. NSIRA finds that CSE has not updated the Minister of National Defence since [*year*] on its relationship with a foreign partner.

2. NSIRA finds that in the context of a joint operation, CSE's analytic exchanges with a partner did not comply with all of CSE's internal policy requirements relating to such exchanges with its partners.

3. NSIRA finds that CSE's applications to the Minister of National Defence for Foreign Intelligence Authorizations did not describe the full extent of CSE's involvement in [*specific activity*].

4. NSIRA finds that CSE did not appropriately apply its Mistreatment Risk Assessment process to information shared with a foreign partner. CSE conducted a mistreatment risk assessment only after having already shared substantial information with the partner.

5. NSIRA finds that CSE did not appropriately justify its mistreatment risk for targets of an operation.

6. [*Finding not releasable in public report*]

7. NSIRA finds that CSE does not have a mechanism to obtain timely and concrete verification of a person's Canadian status in order to verify that it is not directing its activities at Canadians.

8. NSIRA finds that CSE has not developed policies and procedures to govern its participation in [*specific activity*].

9. NSIRA finds that CSE's contributions to operations with its partners are not governed by any written arrangements with operational activities.

10. NSIRA finds that CSE's contributions to operations led by a partner have not been accompanied with the operational planning and risk assessment as described by CSE to the Minister of National Defence.

11. NSIRA finds that CSE does not obtain operational plans or risk assessments developed by its partners leading the operations, nor contributes to the development of these plans or their associated parameters.

12. NSIRA finds that CSE's application for the Authorization did not inform the Minister of National Defence that it intends to conduct testing and evaluation activities under the authority of the Authorization.

NSIRA's recommendations, and CSE response

Recommendation	CSE Response (14 March 2023)
Recommendation 1: CSE should update the Minister of National Defence on of its relationship with a foreign partner.	**Agree.** CSE agrees with this recommendation. CSE concurs and regularly updates the minister on topics of importance, including the status of relationships with international partners. CSE plans to continue providing comprehensive updates to the Minister on its international engagements and relationships with foreign partners, including the named foreign partner.
Recommendation 2: CSE should comply with the Releasable SIGINT Products requirements pursuant	**Agree.** CSE agrees with this recommendation.

Recommendation	CSE Response (14 March 2023)
to the Foreign Intelligence Mission Policy Suite when conducting analytic exchanges with its partners in the performance of all operational activities.	CSE recognizes that despite having robust policies, practices, and procedures, improvements can still be made in outreach and training to mission staff. CSE is working on a comprehensive revision of its operational legal and policy training, and will consider this recommendation when developing its compliance plans for 2023–2024.
Recommendation 3: CSE should describe to the Minister of National Defence the full extent of its participation in any activities when applying for Foreign Intelligence Authorizations.	**Agree.** CSE agrees with this recommendation. CSE will include relevant details to clarify [specific activities] in its next Ministerial Authorization application at a level of detail consistent with Ministerial Authorization applications.
Recommendation 4: CSE must perform a Mistreatment Risk Assessment prior to sharing information with [*country*] in accordance with parameters established with the Minister of National Defence, Minister of Foreign Affairs, and the Privy Council Office in the development of CSE's working arrangement with this partner.	**Agree in principle.** CSE agrees with this recommendation in principle. CSE is of the view that its policy instruments are already clear and that there are already established best practices when sharing information with foreign entities about identifiable individuals. CSE continually seeks to improve both the implementation of internal policies, and the training and internal outreach programs for its analysts. Additionally, it is important to note that there exists a strong mitigating factor in the overarching agreements with [*country*] which contain explicit language regarding how SIGINT may be used, and with explicit prohibitions for purposes that could result in mistreatment.
Recommendation 5: When performing a Mistreatment Risk Assessment, CSE should specify why and how its risk rating applies to each individual implicated in the sharing of information with a foreign partner.	**Agree in principle.** CSE agrees with this recommendation in principle. Since 2011, CSE has continually refined its mistreatment risk assessment process and documentation. In certain cases where an initial assessment has determined that all of the conditions of information sharing will be identical across a category of individuals in an activity, CSE has determined that a group mistreatment risk

Recommendation	CSE Response (14 March 2023)
	assessment appropriately documents the risk profiles for all individuals associated with that activity. In the event that the information sharing conditions change, or specific characteristics related to an individual associated with the activity may change the risk, a separate assessment is conducted. CSE has continued to improve our documentation to ensure that it better reflects the analysis behind the risk assessment and why a rationale would apply to a group of individuals under a single activity. As CSE's operational activities continue to evolve, the mistreatment risk assessment process grows to reflect the requirements of those activities.
Recommendation 6: CSE should ensure that a foreignness assessment is completed prior to commencing collection and reporting on individuals. CSE should also develop policy requirements for the documentation, tracking, and management review of foreignness assessments.	**Agree in principle.** CSE agrees with this recommendation in principle. As part of the SIGINT process, and relying on a combination of policy, administrative, and technological means, CSE already documents a targeting justification demonstrating reasonable grounds to believe that a target is a foreign entity outside Canada. This auditable justification crystallizes the current state of knowledge about the foreignness of a target, at the time of targeting. In addition, as analysts perform their duties and build knowledge about a target, a foreignness assessment persists throughout SIGINT analysis in a process that is guided by the Mission Policy Suite. Each new fragment of information acquired about a target increases the body of knowledge evaluated by an analyst, including more information about a target's foreignness that may not have been available at the time of targeting. If at any point the analyst no longer has reasonable grounds to believe that the target is a foreign entity outside Canada, the analyst must de-target the associated selectors and register a

Recommendation	CSE Response (14 March 2023)
	privacy incident with CSE's Program for Operational Compliance team, who will guide internal processes through any additional required remedial steps, such as purging any collected information. In addition, a citizenship check can also be requested from Immigration, Refugees, and Citizenship Canada (IRCC) if sufficient information is available.
Recommendation 7: CSE should develop a mechanism with Immigration, Refugees and Citizenship Canada, or other federal institutions as appropriate, to facilitate timely and concrete confirmation of the Canadian status of individuals implicated in CSE's operational activities.	**Agree.** CSE agrees with this recommendation. This recommendation was previously put forward in the SCIDA 2020 final report. CSE continues to pursue discussions with IRCC for an information sharing agreement. CSE is reengaging at both working and executive levels to facilitate progress. It should be recognized that in order to produce more accurate results, a citizenship check needs to include specific information regarding an individual target, which is not always available to CSE. In the absence of that information, a citizenship check is not guaranteed to produce conclusive results, and cannot be considered as a concrete confirmation of citizenship status. In addition, it is CSE's understanding that IRCC databases may not capture Canadians born with Canadian citizenship. The citizenship check process and associated timelines are fully within the jurisdiction of IRCC.
Recommendation 8: CSE should develop policies and procedures to govern its participation in [*specific activities*] within the program.	**Agree.** CSE agrees with this recommendation. CSE remains committed to building robust policy frameworks to govern its activities and ensure that its work continues at the highest level of integrity. While at the time of review, policies and procedures specific to the program were still in development, CSE's existing policies and procedures include principles that govern all foreign intelligence activities conducted under CSE authorities, including [*program*].

Recommendation	CSE Response (14 March 2023)
Recommendation 9: CSE should develop written arrangements with its partners implicated in activities, to set the parameters for collaborating on these activities.	**Disagree.** CSE disagrees with this recommendation. CSE has enjoyed a uniquely strong relationship with partners for [*amount of time*]. By leveraging shared capabilities, Canada benefits greatly, magnifying its ability to provide quality information exponentially. The cooperation with our partners means that we [*description*], with procedures in place to manage our interactions. CSE's operations with partners are based on bilateral information sharing and technical cooperation arrangements.
Recommendation 10: When collaborating on an operation with a partner, CSE should prepare an operational plan and conduct a risk assessment associated with the activity with a view to ensuring an operation's alignment with CSE's priorities and risk tolerance levels. CSE should also ensure that parameters and any caveats for the partner's [*specific activity*] be outlined and acknowledged.	**Agree.** CSE agrees with this recommendation. CSE policy outlines that, when conducting SIGINT operations, including joint operations with a partner, the activity be approved via an operational plan and risk assessment in order to exercise an aspect of the CSE mandate. Collaboration that involves [*specific activity*] without participating in the resulting operation does not require operational plans or risk assessments to be created at CSE, but rather at the partner agency conducting the operation and adopting the risk. CSE will, however, ensure that the partner agency is aware of and acknowledges any caveats or parameters.
Recommendation 11: When applying for a Ministerial Authorization, CSE should disclose to the Minister any related testing or evaluation activities that it intends to undertake pursuant to paragraph 23(1)(c) of the CSE Act.	**Disagree.** CSE disagrees with this recommendation. The purpose of a ministerial authorization is to seek authorities for activities that would contravene an Act of Parliament or involve the acquisition of information that interferes with the reasonable expectation of privacy (REP) of a Canadian or any person in Canada. Testing activities, as per s.23(1)(c) of the CSE Act, are not carried out under the authorities of a ministerial authorization if they do not risk contravening an Act of Parliament or do not involve the acquisition

Recommendation	CSE Response (14 March 2023)
	of information that interferes with the REP of a Canadian or any person in Canada. In such cases, it is not required to request authorities to conduct testing activities from the Minister through a ministerial authorization. However, at the Chief's discretion, CSE will inform the Minister of non-ministerial authorization activities through other means. Paragraph 23(1)(c) provides an exception to CSE's prohibition on directing its activities at a Canadian or any person in Canada when conducting testing or evaluating products, software and systems. This means that CSE may conduct these activities which will not be considered directed at a Canadian or any person in Canada. Any foreign intelligence activities, including testing activities, that contravene an Act of Parliament or involve the acquisition of information that interferes with the REP of a Canadian or any person in Canada can only be conducted under the authorities of a ministerial authorization. In such cases, the activities must be conducted under the authorities of an existing ministerial authorization or will require that the Minister issue a new ministerial authorization, and the Minister would be fully informed of the activities being considered before being in a position to approve them.

Department of National Defence and the Canadian Armed Forces Review

Report issued pursuant to section 35 of the NSIRA Act

NSIRA's finding

1. The report contained a finding that, in NSIRA's opinion, certain activities undertaken by the Canadian Armed Forces may not have been in compliance with the law.

Department of National Defence and the Canadian Armed Forces (DND/CAF's) response

DND/CAF recognize the importance of independent, external reviews of the Government of Canada's national security and intelligence activities. We fully support NSIRA's review mandate and take all of its reports seriously.

Upon receipt of NSIRA's section 35 compliance report, DND/CAF conducted a comprehensive analysis and do not agree with NSIRA's opinion. Our analysis supports that the reviewed activities were conducted in accordance with the law within a robust system of oversight and accountability. Furthermore, an earlier independent external review was consistent with our analysis and supported a number of recommendations that were implemented to strengthen the governance framework. The Minister is following the steps in order to meet all the requirements outlined in section 35 of the Act.

Canada Border Services Agency review

Air Passenger Targeting Review

NSIRA's findings

1. The use of Advance Passenger Information and Passenger Name Record data by the Canada Border Services Agency (CBSA) in scenario-based targeting complied with section 107(3) of the *Customs Act*.

2. The CBSA does not document its triaging practices in a manner that enables effective verification of whether all triaging decisions comply with statutory and regulatory restrictions.

3. The CBSA has not consistently demonstrated that an adequate justification exists for its Air Passenger Targeting triaging practices. This weakness in the link between the indicators used to triage passengers and the potential threats or contraventions they seek to identify creates a risk that Air Passenger Targeting triaging practices may be discriminatory.

4. The CBSA's policies, procedures, and training are insufficiently detailed to adequately equip CBSA staff to identify potential discrimination-related risks and to take appropriate action to mitigate these risks in the exercise of their duties.

5. The CBSA's oversight structures and practices are not rigorous enough to identify and mitigate potential discrimination-related risks, as appropriate. This is compounded by a lack of collection and assessment of relevant data.

NSIRA's recommendations, and the CBSA's responses

Recommendation	Response (July 2022)
Recommendation 1: NSIRA recommends that the CBSA document its triaging practices in a manner that enables effective verification of whether all triaging decisions comply with statutory and regulatory restrictions.	**Agree.** The CBSA will complete a review of its air passenger targeting triaging practices to ensure practices are in place which will enable effective verification of compliance with statutory and regulatory restrictions.
Recommendation 2: NSIRA recommends that the CBSA ensure, in an ongoing manner, that its triaging practices are based on information and/or intelligence that justifies the use of each indicator. This justification should be well-documented to enable effective internal and external verification of whether the CBSA's triaging practices comply with its non-discrimination obligations.	**Agree.** While we are satisfied that justification for triaging and targeting practices exist, the CBSA acknowledges that better documentation practices could be implemented to enable effective internal and external verification of whether the CBSA's triaging practices comply with its non-discrimination obligations. The CBSA's Scenario Based Targeting Governance Framework will be updated to include information and/or intelligence that justifies the use of each indicator. Annual reviews of scenarios will continue to be conducted and documented to confirm that each active scenario is supported by recent and reliable intelligence.
Recommendation 3: NSIRA recommends that the CBSA ensure that any Air Passenger Targeting-related distinctions on protected grounds that are capable of reinforcing, perpetuating, or exacerbating a disadvantage constitute a reasonable limit on travellers' equality rights under the Charter.	**Agree.** The CBSA will review its air passenger targeting practices to ensure that distinctions based on protected grounds are reasonable and can be demonstrably justified in the border administration and enforcement context.
Recommendation 4: NSIRA recommends that the CBSA develop more robust and regular oversight for	**Agree.** The CBSA acknowledges that policies, procedures, training, and other guidance, as

Recommendation	Response (July 2022)
Air Passenger Targeting to ensure that its practices are not discriminatory. This should include updates to the CBSA's policies, procedures, training, and other guidance, as appropriate.	appropriate can be improved to ensure robust and regular oversight for Air Passenger Targeting to ensure that its practices are not discriminatory. The CBSA will complete a review of its policies, procedures, guidelines and training to ensure practices are not discriminatory.
Recommendation 5: NSIRA recommends that the CBSA start gathering and assessing the necessary data to identify, analyze, and mitigate discrimination-related risks. This includes disaggregated demographic data, data on the effects of Air Passenger Targeting on secondary examinations that may be apparent from related human rights complaints, and data on a baseline comparator group.	**Agree.** To that end, the CBSA is taking deliberate steps to develop its capacity to capture and analyze reliable and accurate data in non-intrusive ways. The Agency is working on developing standard and consistent positions and frameworks on the collection, use, management and governance of disaggregated data, developing metrics and indicators to measure the impact of decisions and policies on different groups; using data to build more inclusive and representative policies and strategies, and; identifying possible discrimination and bias.

Multi-departmental reviews

Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2021

NSIRA's findings

1. NSIRA finds that, in 12 out of 13 disclosures, Global Affairs Canada demonstrated that it satisfied itself as to the contribution of the information to the recipient institution's responsibilities in respect of activities that undermine the security of Canada, as required under paragraph 5(1)(a) of the SCIDA.

2. NSIRA finds that, without first conducting the analysis under paragraph 5(1)(a) of the SCIDA, departments risk disclosing information that does not pertain to the national security mandate of the recipient institution or to activities that undermine the security of Canada.

3. NSIRA finds that, in 1 of 13 disclosures, Global Affairs Canada consulted on more information than necessary to obtain confirmation from CSIS that the disclosure contributed to its mandate and was linked to activities that undermine the security of Canada.

4. NSIRA finds that, in 10 out of 13 disclosures, Global Affairs Canada demonstrated that it satisfied itself that the disclosure will not affect any person's privacy interest more than reasonably necessary in the circumstances, as required under paragraph 5(1)(b) of the SCIDA.

5. NSIRA finds that 2 of 13 disclosures did not contain the accuracy and reliability statements as required by subsection 5(2) of the SCIDA.

6. NSIRA finds that Global Affairs Canada training on the SCIDA lacks sufficient illustrative examples required to provide employees with adequate guidance to fulfill their obligations under the SCIDA.

NSIRA's recommendations, and government response

Recommendation	Response (February 14th, 2023)
Recommendation 1: NSIRA recommends that consultations be limited to the information necessary to obtain confirmation from the potential recipient that the information contributes to its mandate and is linked to activities that undermine the security of Canada.	**Agree.** Public Safety's Step-by-Step SCIDA Guide 2022 ("SCIDA Guide 2022") was updated and distributed to federal institutions in October 2022. Many of the updates to the SCIDA Guide 2022, that were based on practitioner feedback, directly address this recommendation. The updated SCIDA Guide 2022 specifies that preliminary consultations prior to a disclosure should only include general information to ensure that SCIDA thresholds are met before the disclosing institution proceeds with the disclosure. In addition, SCIDA training material was updated in September 2022 with a renewed emphasis on the need for disclosing institutions to strictly limit the information communicated with recipient institutions during preliminary consultations. Multiple SCIDA trainings have been delivered to federal institutions using the new material. Public Safety will continue to work with federal institutions to provide them with access to training, guidance and other useful resources on the use of the SCIDA. Given the focus of this

Recommendation	Response (February 14th, 2023)
	review, Public Safety will work closely with Global Affairs Canada to address this recommendation.
Recommendation 2: NSIRA recommends that in order to provide the most valuable and meaningful context for the recipient institution, accuracy and reliability statements should be clear and specific to the circumstances of the disclosure.	**Agree.** Statements regarding the accuracy of the information and the reliability of the manner in which it was obtained are an essential part of the disclosure process. To ensure greater compliance with this requirement, the SCIDA Guide 2022 and its related templates, as well as the updated SCIDA training material, emphasize the importance of providing statements on the accuracy of the information and reliability of the manner in which it was obtained that are clear and specific to the circumstances of the disclosure. Public Safety will continue to provide SCIDA training and guidance to federal institutions to highlight the requirement for statements of accuracy and reliability that are clear, complete, accurate and do not include formulaic language in support of disclosures under the SCIDA.
Recommendation 3: NSIRA recommends that all disclosing departments contemporaneously prepare descriptions of the information that was relied on to satisfy themselves that disclosures were authorized under the SCIDA.	**Agree.** Record keeping is an essential component of the SCIDA, and records of disclosures must include an appropriately robust description of the information relied upon to satisfy the disclosing institution that the disclosure meets the thresholds of the SCIDA. The SCIDA Guide 2022 includes templates that support federal institutions with their record-keeping requirements. This includes sections where disclosing institutions must prepare and maintain records that set out a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under the SCIDA. While paragraph 9(1)(e) of the SCIDA does not explicitly require departments to contemporaneously prepare descriptions of the information related to SCIDA disclosures, Public Safety takes note of NSIRA's recommendation to do so in a timely manner.

Recommendation	Response (February 14th, 2023)
	Public Safety will continue to provide SCIDA training and guidance to federal institutions to highlight their recordkeeping obligations to ensure that all disclosures are authorized under the SCIDA and assist them in understanding their authorities for requesting and disclosing information under the Act.
Recommendation 4: NSIRA recommends that additional illustrative examples and scenarios be included in the SCIDA training, including for disclosure threshold requirements, accuracy and reliability statements and record-keeping requirements.	**Agree.** SCIDA training material was updated in September 2022 with multiple illustrative examples and case studies that provide further details on how to apply the disclosure threshold requirements, accuracy and reliability statements and record-keeping requirements. SCIDA training sessions have been delivered to federal institutions using the new material. Given the focus of this review, Public Safety will work closely with Global Affairs Canada to address this recommendation.

Review of departmental implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2021

NSIRA's findings

1. NSIRA finds that the Canada Border Services Agency and Public Safety Canada still have not fully implemented an ACA framework and supporting policies and procedures are still under development.
2. NSIRA finds that from January 1, 2021, to December 31, 2021, no cases under the ACA were escalated to deputy heads in any department.
3. NSIRA finds that the RCMP has a robust framework in place for the triage of cases pertaining to the ACA.
4. NSIRA finds that the RCMP's Foreign Information Risk Advisory Committee (FIRAC) risk assessments include objectives external to the requirements of the Orders in Council, such as the risk of not exchanging information.

5. NSIRA finds that the RCMP use of a two-part risk assessment, that of the country profile and that of the individual to determine if there is a substantial risk, including the particular circumstances of the individual in question within the risk assessment is a best practice.

6. NSIRA finds that the RCMP does not have a centralized system of documenting assurances and does not regularly monitor and update the assessment of the reliability of assurances.

7. NSIRA finds that the RCMP does not regularly update or have a schedule to update its Country and Entity Assessments. In many cases these assessments are more than four years old and are heavily dependent on an aggregation of open-source reporting.

8. NSIRA finds that information collected through the Liaison Officer in the course of an operation is not centrally documented such that it can inform future assessments.

9. NSIRA finds that FIRAC members concluded that the information sharing would result in a substantial risk of mistreatment that could not be mitigated. The Assistant Commissioner determined that it may be mitigated. This amounts to a disagreement between officials or a situation where "officials are unable to determine whether the risk can be mitigated".

10. NSIRA finds that the Assistant Commissioner's rationale for rejecting FIRAC's advice did not adequately address concerns consistent with the provisions of the Orders in Council. In particular, NSIRA finds that the Assistant Commissioner erroneously considered the importance of the potential future strategic relationship with a foreign entity in the assessment of potential risk of mistreatment of the individual.

11. NSIRA finds that Global Affairs Canada is now strongly dependent on operational staff and Heads of Mission for decision-making and accountability under the ACA.

12. NSIRA finds that Global Affairs Canada has not demonstrated that all of its business lines are integrated into its framework under the ACA.

13. NSIRA finds that Global Affairs Canada has not made ACA training mandatory for all staff across relevant business lines. This could result in staff being involved in information exchanges without the proper training and knowledge of the implications of the ACA.

14. NSIRA finds that Global Affairs Canada has not regularly updated its Human Rights Reports. While many were updated during the 2021 review year, more than half have not been updated since 2019. This is particularly problematic when departments and agencies rely on these reports as a key source in assessing risk related to the ACA.

15. NSIRA finds that Global Affairs Canada does not have a standardized centralized approach for the tracking and documentation of assurances.

NSIRA's recommendations

Recommendation
Recommendation 1: NSIRA recommends that the RCMP establish a centralized system to track caveats and assurances provided by foreign entities and where possible to monitor and document whether said caveats and assurances were respected.
Recommendation 2: NSIRA recommends that in cases where the RCMP Assistant Commissioner disagrees with FIRAC's recommendation not to share the information, the case be automatically referred to the Commissioner.
Recommendation 3: NSIRA recommends that the assessment of substantial risk be limited to the provisions of the Orders in Council - namely the substantial risk of mistreatment and whether the risk may be mitigated - and external objectives such as fostering strategic relationships should not factor into this decision-making.
Recommendation 4: NSIRA recommends that FIRAC recommendations are referred to an Assistant Commissioner who is not responsible for the branch from which the case originates.
Recommendation 5: NSIRA recommends that GAC ensure that accountability for compliance with the ACA clearly rests with the Avoiding Mistreatment Compliance Committee.
Recommendation 6: NSIRA recommends that GAC conduct a formal internal mapping exercise of other possibly implicated business lines to ensure it is meeting its obligations set out in the ACA.
Recommendation 7: NSIRA recommends that GAC make ACA training mandatory for all rotational staff.
Recommendation 8: NSIRA recommends that GAC ensure countries' Human Rights Reports are updated more regularly to ensure evolving human rights related issues are captured.
Recommendation 9: NSIRA recommends that GAC establish a centralized system to track caveats and assurances provided by foreign entities and document any instances of non-compliance for use in future risk assessments.

Review arising from the Federal Court's decision in 2020 FC 616, rebuilding trust: reforming the CSIS warrant and Department of Justice legal advisory processes

This review was approved in 2022. Under section 38 (1) of the NSIRA Act, NSIRA is therefore obliged to report on its findings and recommendations as part of its annual report for the calendar year 2022. A summary of this review is available in NSIRA's Annual Report 2021.

NSIRA's findings

1. NSIRA finds that the legal advice-seeking and giving process, and resource constraints at the Department of Justice's National Security Litigation and Advisory Group (NSLAG) contribute to considerable delays, [*description of timeline*].

2. NSIRA finds that Justice legal opinions have sometimes been prepared without sufficient attention to the audience that needs to understand and act on them. Opinions have been focused on assessing legal risk, often late in the development of a CSIS activity, with limited effort made to propose alternative and legally sustainable means of arriving at the intended objective.

3. NSIRA finds that the Justice Legal Risk Management Framework is misunderstood at the working level at CSIS and further that it does not provide an appropriate framework for the unequivocal communication of unlawful conduct to CSIS.

4. NSIRA finds that difficulties in acquiring prompt and relevant legal advice have contributed to [*discussion of the detrimental effects on and risks to operations*] that may require legal advice. In consequence, the manner in which NSLAG has provided legal advice to CSIS has often not met the needs of CSIS operations.

5. NSIRA finds that Justice does not generate the necessary business analytics to track its service delivery performance to CSIS.

6. NSIRA finds that Justice has acknowledged that internal silos at NSLAG between the advisory and litigation wings have sometimes left warrant counsel unaware of emerging legal issues and that Justice has taken steps to resolve these issues.

7. NSIRA finds that Justice has committed to improve its advice-giving to CSIS, including moving toward "road map" style legal advice that involves working collaboratively and iteratively with CSIS to achieve operational goals within the bounds of the law.

8. NSIRA finds that CSIS has not always shared all relevant information with NSLAG, prompting a degree of mistrust and limiting Justice's ability to provide responsive legal advice.

9. NSIRA finds that CSIS has a history of quick reforms, followed by neglect, high turnover of personnel leading to a loss of institutional knowledge, and resourcing that did not match stated priorities. CSIS does not track or measure the outcome of past reforms adequately and has no performance metrics for assessing success.

10. NSIRA finds that CSIS policies have not kept pace with operational reality, as they are often vague, dated, overlapping and contradictory. The absence of clear policy creates legal doubt or concerns, and gives rise to disparate interpretations of legal and operational standards.

11. NSIRA finds that there is little common understanding regarding the process or basis on which a warrant is prioritized. Frequent shifts in this process of prioritization have added to operational uncertainty. The prioritization process has made it very difficult to bring novel issues to the Court with the goal of addressing legal ambiguities through court decisions.

12. NSIRA finds that the actors involved in the warrant process do not have a common understanding of the rationale for each of the [*multiple*] of steps in the overarching warrant application scheme and are not always sure what role each approval step plays.

13. NSIRA finds that the proliferation of process in seeking warrants has created a system of diluted accountability widely regarded as slow and unwieldy, with delays caused by multiple levels of approval.

14. NSIRA finds there is no regular feedback process in which explanations for warrant-related decisions made at one level filter back to other levels. The absence of feedback is especially acute for the regional investigators.

15. NSIRA finds that often, the sole means to address legal uncertainty is to bring legal questions to the Federal Court through warrant applications. In consequence, an unwieldy warrant process makes resolution of legal doubt more difficult.

16. NSIRA finds that CSIS has struggled to ensure that all information material to the credibility of sources is properly contained in warrant applications. This “recurring omissions” problem stems from a misunderstanding of the Federal Court’s role in assessing the credibility of sources and from the presence of multiple, siloed information management systems. CSIS has undertaken reforms, but work remains to implement long-term sustainable solutions.

17. NSIRA finds that the Affiant Unit constitutes a vital and laudable reform within CSIS. However, the Affiant Unit is currently at risk of collapse. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS’s mission. The benefits of the Affiant Unit are currently in jeopardy because of governance, human resource, and training deficiencies.

18. NSIRA finds that the Affiant Unit's placement in the [*Name*] branch is not commensurate with its functions and importance. This governance anomaly most likely contributes to administrative hurdles and resource challenges faced by the Affiant Unit.

19. NSIRA finds that without a functional Affiant Unit able to produce timely and accurate warrant applications, CSIS puts at risk access to warrants and the information collected under them.

20. NSIRA finds that the "independent counsel" role falls short of creating a thorough challenge function.

21. NSIRA finds that the CSIS regional warrants coordinators have not received sufficient training enabling them to translate the contents of the warrants into advice on proper warrant execution.

22. NSIRA finds that CSIS lacks long-term training programs for Intelligence Officers.

23. NSIRA finds that CSIS has failed to provide systematic training programs for "non-Intelligence Officers."

24. NSIRA finds that the CSIS's Learning and Development Branch has not been sufficiently resourced to develop and administer comprehensive training programs, especially in specialized areas not covered by the training offered for Intelligence Officers early in their career.

25. NSIRA finds that CSIS and Justice are at risk of not being able to fulfill their respective mandates. No one reform is likely to succeed unless each is pursued as part of a coherent package. No package will succeed unless backed by prioritization at senior levels, and the stable provision of resources, including people with the means and institutional knowledge to see reforms through. And no reform initiative will succeed unless accompanied by clear performance indicators, measured and analyzed regularly to track progress.

NSIRA's recommendations and departmental responses

Recommendation	Departmental response (March 29, 2022)
Recommendation 1: NSIRA recommends that Justice pursue its commitment to reforming the manner of providing legal advice to CSIS, and its stated commitment to "road map"-style advice as a best practice. In support of this objective and the	**Agree.** Prior to NSIRA issuing its report, Justice Canada has been working on a number of measures concerning policies and practices in the provision of legal services to CSIS. These measures include activities related to the duty of

Recommendation	Departmental response (March 29, 2022)
provision of timely, operationally relevant advice, NSIRA further recommends that Justice implement the following: • Whether through an expanded "office hours" and liaison counsel program or otherwise, NSLAG must develop a legal support service operating full time, staffed by experienced lawyers empowered to provide operational advice in real time on which CSIS officers can rely, on the basis of settled Justice positions on recurring legal issues, accessible directly to CSIS officers across all regional offices and at all levels. • NSLAG develop a concise reference tool with its position on recurring issues and most common legal authorities invoked and make the tool accessible to counsel to support their real-time advice. • To minimize the need to resort to the formalized legal advice-seeking process, NSLAG (in coordination with CSIS) must involve counsel with CSIS officers at the early stage of the planning of key or novel operations and throughout their entire operational lifecycle to case-manage an iterative legal guidance process.	candour and the warrant acquisition process, best practices in the delivery of legal services, advising CSIS on legal risks associated with its operations, the sharing of information in the national security context, and tracking and responding to key performance indicators related to the delivery of legal services. Justice is committed to improving the manner of providing legal services and ensuring practical and timely legal services. The measures undertaken to date and further measures underway support a coordinated approach for legal services, striking the right balance of resources across corporate and operational priorities. This includes providing legal advice in a more accessible, iterative manner, and supporting Counsel through interactive training to better understand and support their work in a proactive manner. Justice and CSIS working together in an integrated fashion ensures that counsel are involved throughout an operation's life-cycle, including the early stages. Early integration into operational planning supports the provision of timely and relevant legal advice as operations progress. Justice has already modified its liaison counsel model. Liaison counsel are experienced counsel designated to support CSIS officers across regional offices and particular operations. Enhancements to the role have resulted in liaison counsel providing timely and focused advice, supporting operational imperatives, and identifying trends and issues of concern to develop guidance documents and other practical tools. Justice is developing a suite of practical tools and legal service delivery mechanisms to support CSIS. These include: • a user-friendly blog that describes relevant legal issues and concepts in plain-language

Recommendation	Departmental response (March 29, 2022)
	and with a practical application to CSIS's work; • a field guide for the practical application of legal concerns to CSIS's operations that can be used by officers in the field and in real time; • interpretation and guidance documents; and, • knowledge management tools ensuring counsel can access legal precedents and interpretations.
Recommendation 2: NSIRA recommends that NSLAG (in coordination with CSIS) develop Key Performance Indicators to measure the delivery of legal services to CSIS.	**Agree.** Justice has developed business metrics to measure service delivery performance. Justice will continue to work with CSIS to invest in resources to conduct detailed business analytics to enhance the provision of legal services and make improvements to the existing system. Client feedback surveys are undertaken regularly.
Recommendation 3: NSIRA recommends that CSIS and Justice should include in their training programs interactive scenario-based training developing the operational intelligence activities expertise of NSLAG counsel and the legal knowledge of CSIS operational staff.	**Agree.** Justice has worked with CSIS to develop and deliver interactive scenario-based training and is committed to continuing that involvement. Cross-reference recommendations 14 and 18.
Recommendation 4: To ensure Justice is able to give meaningful and responsive legal advice as recommended in recommendation #1, NSIRA recommends that CSIS invite Justice counsel to sit at the table at all stages of the lifecycle of key and novel operations, and that it fully and frankly brief counsel on operational objectives, intent, and details.	**Agree.** As set out above, Justice is working with CSIS to be involved sooner and more continuously across the lifecycle of operations to provide timely, focused and iterative legal services.
Recommendation 5: NSIRA recommends that Justice's advice-giving must clearly and unequivocally communicate advice on the unlawfulness of client conduct, whether criminal or otherwise.	**Agree.** Justice is currently undertaking a review of its legal risk framework in order to improve both how legal risk is assessed, and also how risks are communicated to clients.

Recommendation	Departmental response (March 29, 2022)
Recommendation 6: NSIRA recommends that CSIS adopt, and share internally, clear criteria for the warrant prioritization process.	**Agree.** CSIS will further refine the warrant prioritization process and work to set clear criteria.
Recommendation 7: NSIRA recommends that CSIS establish a new warrant process eliminating steps that do not make a significant contribution to a more accurate application. The process should assign clear lines of responsibility for the production of accurate applications. The reformed system should ensure that delays associated with managerial approvals are minimized, and that time is reallocated to those steps contributing to the preparation of the accurate applications.	**Agree.** Work on implementation is underway. CSIS and Justice are committed to streamlining warrant applications, templates, and requests as part of broader modernisation objectives.
Recommendation 8: NSIRA recommends that CSIS integrate the regional stakeholders (including the implicated investigators) at every key milestone of the warrants process.	**Agree.** CSIS has already undertaken related improvements to address this recommendation, including through the updated Affiant Unit business approach to warrant acquisition, which now includes regional stakeholders.
Recommendation 9: NSIRA recommends that CSIS adopt policies and procedures governing the reformed warrant process that clearly outlines the roles and responsibilities of each participant and the objective of each step in the warrant process and that these policies be kept current as the process evolves.	**Agree.** The revised CSIS Justice Joint Policy on Duty of Candour and the associated guidance document outline the role of all CSIS employees (not just the affiants) in ensuring that disclosure obligations to the Court are met. In addition, CSIS has developed a s.21 warrant policy and the drafting of the related procedure is underway. In 2020 and 2021, CSIS provided Duty of Candour training to all operational employees through a special project.
Recommendation 10: To address the seeming inevitability of "recurring omissions", NSIRA recommends that CSIS prioritize the development of [*an improved*] system for human source information management. CSIS should also continue initiatives meant to ensure that source handlers are assiduous in documenting and then reporting in source precis information going to credibility. Even with these reforms, the Affiant Unit should adopt procedures for verifying the information prepared by the regions.	**Agree.** The recommendation endorses a CSIS initiative already underway. An Action Plan approved by the Executive in January 2021 identified the requirement, and CSIS stakeholders are advancing this initiative. CSIS developed a comprehensive requirements package, and identified a potential technical solution. The complexity of the technical development process means this will be a long process.

Recommendation	Departmental response (March 29, 2022)
Recommendation 11: NSIRA recommends that CSIS recognize the importance of the Affiant Unit by assigning affiants and analysts an employment classification congruent with their responsibilities.	**Agree.** CSIS has addressed this recommendation by classifying affiants at one level above the Intelligence Officer working level to recognize the complexity of their work and to attract/retain candidates. A competitive competition process is underway to staff the affiant positions and is anticipated to be completed by the end of March 2022.
Recommendation 12: NSIRA recommends that CSIS should create an Affiant Branch reporting directly to the CSIS Director.	**Disagree.** The Service notes the concerns raised by the committee in its report regarding the Affiant's Unit current placement in the organization's hierarchy. This said, throughout the course of this review, CSIS has invested heavily in the Affiant Unit and its employees and has made significant changes to the warrant process and its governance. The Service is confident that these changes will be sufficient to address the concerns that resulted in this finding and recommendation, particularly as it relates to observations related to administrative and human resource challenges. In addition, the current placement of the Affiant Unit with other units with corresponding responsibilities for warrant acquisition best facilitates the provision of ongoing guidance and advice throughout the warrant lifecycle to ensure compliance and duty of candour obligations are met. Given its importance, CSIS commits to ongoing monitoring and evaluation of the Affiant Unit to ensure the concerns highlighted in the report do not re-occur.
Recommendation 13: NSIRA recommends that CSIS urgently resource the Affiant Unit to meet its responsibilities and ensure its sustainability. In deciding the size of the Affiant Unit, CSIS should assess how many warrants an affiant team might reasonably complete every year.	**Agree**. In line with the recommendation, CSIS already increased the resourcing of the Affiant Unit and approved changes to the organizational chart in March 2021. As noted above, a staffing action is currently underway that aims to create a pool of qualified candidates which can be leveraged to help increase the Affiant Unit's capacity.
Recommendation 14: NSIRA recommends that CSIS, in consultation with Justice, develop a	**Agree**. CSIS intends to provide fulsome training to the affiant unit, as recommended. In late 2021,

Recommendation	Departmental response (March 29, 2022)
comprehensive training course for all affiants and analysts, codifying best practices and methods for members of the Affiant Unit.	initial consultations were held to identify appropriate training. Unfortunately, the pandemic has disrupted training efforts. Justice is supporting CSIS in the development and delivery of all comprehensive and practical training for all those working on warrant applications. Cross-reference recommendations 3 and 18.
Recommendation 15: NSIRA recommends that NSLAG be staffed by a complement of counsel and support personnel sufficient to ensure that CSIS operations are not impeded by resource limitations at NSLAG.	**Agree**. Justice and CSIS will continue to work together on resources and staffing issues.
Recommendation 16: NSIRA recommends that the function of the Independent Counsel as performed by National Security Group counsel at the Department of Justice should be eliminated, in favour of a new challenge function, analogous to the role a defence lawyer would play were warrants subject to an adversarial process, situated at Public Safety and supported by the Public Safety vetting team, and performed by a knowledgeable lawyer from the Public Prosecution Service of Canada, the private sector, or elsewhere, who is independent from Justice management and not otherwise involved in CSIS warrant applications.	**Agree**. Public Safety will develop an enhanced vetting function, housed in Public Safety Canada, that reflects the principles and objectives set out by NSIRA. Public Safety Canada will develop the enhanced vetting function as part of the CSIS warrant acquisition process such that it provides a meaningful challenge function without adding undue complexity or delay. While this work is underway, Public Safety Canada will take steps to strengthen warrant vetting on an interim basis.
Recommendation 17: NSIRA recommends that CSIS regional warrants coordinator positions receive adequate training, and that CSIS professionalize the position and enable warrant coordinators to more effectively translate the content of warrants into advice on warrant execution.	**Agree**. CSIS acknowledges the importance of training and of centers of expertise. CSIS is determining training requirements.
Recommendation 18: NSIRA recommends that CSIS adequately resource and regularly deliver evergreen scenario-based training programs for all CSIS employees, including:	**Agree**. CSIS is committed to improving the training offered to all of its employees, as recommended. Scenario-based training, which helps employees understand the application of policies and

Recommendation	Departmental response (March 29, 2022)
• annual, comprehensive, warrant training for all operational employees; • specialized onboarding training for all employees not part of the Intelligence Officer program; and • continued long-term training for all specialized personnel.	procedures, is now an integral part of operational training, which includes the development of an annual operational workshop. A recently approved business case will significantly increase staffing in Learning & Development to further enable training of CSIS employees. This business case includes the creation of a new position responsible for developing an enhanced onboarding for all newly hired employees, as well as the creation of new positions to create and deliver additional learning opportunities for all operational employees. Cross-reference recommendations 3 and 14.
Recommendation 19: The recommendations within this review should be treated as a coherent package and that progress and outcomes in implementing these recommendations be tracked, allowing management, the Ministers of Public Safety and of Justice, and NSIRA, to assess the efficacy of reforms and course-correct if necessary.	**Agree.** PS, CSIS, and Justice are committed to taking a holistic approach to the implementation of the recommendations and will track and course correct as required in this complex operating environment.
Recommendation 20: The full classified version of this report be shared with the designated judges of the Federal Court.	**Partially agree**. The Attorney General of Canada has shared the full report, redacted for solicitor-client privilege, with the designated judges of the Federal Court of Canada.

Annex D: Statistics on complaints investigations

January 1, 2022, to December 31, 2022

INTAKE INQUIRIES	75	
New complaints filed	**30**	
National Security and Intelligence Review Agency Act (NSIRA Act), section 16, Canadian Security and Intelligence Service (CSIS) complaints	22	
NSIRA Act, section 17, Communications Security Establishment (CSE) complaints	2	
NSIRA Act, section 18, security clearances	3	
NSIRA Act, section 19, Royal Canadian Mounted Police (RCMP) referred complaints	3	
NSIRA Act, section 19, *Citizenship Act*	0	
NSIRA Act, section 45, Canadian Human Rights Commission (CHRC) referrals	0	
Accepted jurisdiction to investigate	**6**	
	Accepted:	**Declined:**
NSIRA Act, section 16, CSIS complaints	3	16
NSIRA Act, section 17, CSE complaints	0	1
NSIRA Act, section 18, security clearances	1	1
NSIRA Act, section 19, RCMP referred complaints	2	3
Total	6	24
Active investigations (at the time of writing)	**19**	
NSIRA Act, section 16, CSIS complaints	9	
NSIRA Act, section 17, CSE complaints	0	
NSIRA Act, section 18, security clearances	4	
NSIRA Act, section 19, RCMP referred complaints	6	
NSIRA Act, section 45, CHRC referrals	0	

Total investigations closed	**65**			
	Abandoned	Final report	Resolved informally	Withdrawn
NSIRA Act, section 16, CSIS complaints	1	0	0	3
NSIRA Act, section 17, CSE complaints	0	0	0	0
NSIRA Act, section 18, security clearances	0	1	0	0
NSIRA Act, section 19, RCMP referred complaints	0	2	0	0
NSIRA Act, section 45, CHRC referrals	0	58	0	0
Total	1	61	0	3

Endnotes

[1] *National Security and Intelligence Review Agency Act* (S.C. 2019, c. 13, s. 2) (NSIRA Act): https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html

[2] For further information on NSIRA's mandate please see our website and previous annual reports.

[3] Civilian Review and Complaints Commission for the RCMP website: https://www.crcc-ccetp.gc.ca/

[4] *Anti-terrorism Act,* SC 2015, c. 20.

[5]The 29 applications submitted by CSIS to the Federal Court in 2022 (including the 28 section 21 applications noted in Table 1) 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 subjected 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, Public Safety Canada, the Communications Security Establishment and the Royal Canadian Mounted Police (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.

[6] *CSIS Act,* section 2 defines threats to national security.

[7] Report of the Events Related to Maher Arar, Factual Background Vol I, note 10.

[8] Amendments to the CSIS Act – Data Analytics Backgrounder, CSIS, 2020 07 18.

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

[10] This review is currently undergoing the releasability process and will be published on a future date.

[11] As of the fourth quarter of fiscal year 2021–22, CSE stopped differentiating between the Privacy Incidents File and Minor Procedural Errors File, as incidents in both files fit the same CSE definition of a privacy incident. Procedural errors are now reported within the Privacy Incidents File.

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

[13] *Security of Canada Information Disclosure Act*, S.C. 2015, c. 20, s. 2, [SCIDA] https://laws.justice.gc.ca/eng/acts/S-6.9. SCIDA came into force on 21 June 2019. SCIDA's predecessor, the *Security of Canada Information Sharing Act*, was in force from 1 August 2015 to 20 June 2019.

[14] https://nsira-ossnr.gc.ca/review-of-departmental-frameworks-for-avoiding-complicity-in-mistreatment-by-foreign-entities-nsira-review

[15] Text that has been redacted for the purposes of s.52 (1) of the NSIRA Act has been replaced by summary language contained within square brackets, e.g., [*summary*]